

蜜罐网络运行方法、装置、设备及存储介质

相关申请的交叉引用

本公开要求于 2022 年 4 月 7 日在中国知识产权局提交的申请号为 No. 202210373820.X，标题为“蜜罐网络运行方法、装置、设备及存储介质”的中国专利申请的优先权，通过引用将该中国专利申请公开的全部内容并入本文。

技术领域

本公开涉及网络安全技术领域，尤其涉及一种蜜罐网络运行方法、装置、设备及存储介质。

10 背景技术

随着互联网行业的快速发展，网络环境遭受入侵攻击的事件也在日渐升高，因此催生了基于蜜罐网络的防御产品，通过在业务子网内部署蜜罐产品，用来伪装脆弱易被攻击的服务，当攻击者访问蜜罐服务时，触发告警。由于蜜罐产品生成的蜜罐网络，与当前业务子网环境毫无关联，并且考虑到整个业务子网的安全性，蜜罐产品所生成的蜜网环境往往都需要与业务子网相隔离，甚至将蜜网直接部署到云服务器上。

发明内容

本公开提供了一种蜜罐网络运行方法、装置、设备及存储介质。

20 根据本公开的第一方面，提供了一种蜜罐网络运行方法，包括：获取业务机器的攻击流量；将攻击流量转发至业务机器对应的蜜罐容器，其中，蜜罐容器的容器地址与业务机器的业务地址相同，业务地址为业务机器的网络地址，容器地址为蜜罐容器的网络地址；返回蜜罐容器生成的虚拟数据，其中，虚拟数据为攻击流量请求的数据，虚

拟数据包括容器地址。

根据本公开提供的一种蜜罐网络运行方法，获取业务机器的攻击流量之前，还包括：获取业务机器的所述业务地址；根据业务地址，创建业务机器对应的蜜罐容器。

- 5 根据本公开提供的一种蜜罐网络运行方法，获取所述业务机器的业务地址，包括：获取探针传输的业务地址，其中，探针位于业务机器，探针用于获取并转发业务机器的业务地址；获取业务机器的攻击流量，包括：获取探针传输的攻击流量，其中，探针还用于转发访问业务机器的攻击流量。

- 10 根据本公开提供的一种蜜罐网络运行方法，获取所述业务机器的业务地址之前，还包括：获取业务子网的业务网段，其中，业务网段包括业务子网占用的至少一个所述网络地址；根据业务网段，设置应用容器引擎，其中，应用容器引擎用于根据业务网段中的网络地址，创建网络地址对应的蜜罐容器；根据业务地址，创建业务机器对应的蜜罐容器，包括：确定业务地址属于业务网段后，调用应用容器引擎创建业务机器对应的蜜罐容器。

- 20 根据本公开提供的一种蜜罐网络运行方法，根据业务地址，创建业务机器对应的蜜罐容器之前，包括：获取构建业务机器对应的蜜罐容器的蜜罐自定义指令，其中，蜜罐自定义指令包括蜜罐容器的执行方式和服务类型；根据业务地址，创建业务机器对应的蜜罐容器，包括：根据业务地址，以蜜罐自定义指令中的执行方式和服务类型，创建业务机器对应的蜜罐容器，其中，蜜罐服务包括以服务类型建立的虚拟服务；将攻击流量转发至业务机器对应的蜜罐容器之后，还包括：根据攻击流量，以执行方式执行虚拟服务。

- 25 根据本公开提供的一种蜜罐网络运行方法，获取探针传输的业务地址，包括：获取至少一个探针分别传输的至少一个业务地址，其中，

- 至少一个探针分别位于至少一个业务机器；根据业务地址，创建业务机器对应的蜜罐容器，包括：根据至少一个业务地址，创建至少一个业务机器分别对应的蜜罐容器；获取探针传输的攻击流量，包括：获取至少一个探针传输的、分别针对至少一个业务机器的攻击流量；将
- 5 攻击流量转发至业务机器对应的蜜罐容器，包括：将分别针对至少一个业务机器的攻击流量，分别转发至至少一个业务机器分别对应的蜜罐容器。

- 根据本公开提供的一种蜜罐网络运行方法，根据至少一个业务地址，创建至少一个业务机器分别对应的蜜罐容器之后，还包括：以预设
- 10 时长为周期，将心跳信息发送给 N 个待监测探针，其中，以预设时长为周期发送心跳信息给每一个待监测探针，其中，待监测探针指的是与蜜罐宿主机连接的探针， N 个待监测探针分别位于 N 个业务机器， N 为大于或等于 1 的整数；获取 M 个待监测探针返回的反馈信息，确定 M 个待监测探针为活动探针，其中，活动探针为正常运行
- 15 的探针， M 为大于或等于 1，且小于或等于 N 的整数；确定 M 个活动探针中的至少一个新增加探针，其中，新增加探针为未创建对应蜜罐容器的新增加业务机器对应的探针；分别获取每一个新增加探针传输的新增加业务地址；根据每一个新增加业务地址，分别建立每一个新增加业务机器对应的蜜罐容器。

- 20 根据本公开的第二方面，提供了一种蜜罐网络运行装置，包括：获取模块，用于获取业务机器的攻击流量；转发模块，用于将攻击流量转发至业务机器对应的蜜罐容器，其中，蜜罐容器的容器地址与业务机器的业务地址相同，业务地址为业务机器的网络地址，容器地址为蜜罐容器的网络地址；返回模块，用于返回蜜罐容器生成的虚拟数
- 25 据，其中，虚拟数据为攻击流量请求的数据，虚拟数据包括容器地址。

根据本公开的第三方面，提供了一种电子设备，包括存储器、处

理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行程序时实现如上述任一种所述蜜罐网络运行方法的步骤。

根据本公开的第四方面，提供了一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现如上述任

5 一种所述蜜罐网络运行方法的步骤。

本公开提供的蜜罐网络运行方法、装置、设备及存储介质，获取业务机器的攻击流量之后，将攻击流量转发至业务机器对应的蜜罐容器，其中，蜜罐容器的容器地址与业务机器的业务地址相同，业务地址为业务机器的网络地址，容器地址为蜜罐容器的网络地址；最后返

10 回蜜罐容器生成的虚拟数据，其中，虚拟数据为攻击流量请求的数据，虚拟数据包括容器地址。通过上述过程构建的蜜罐网络中，蜜罐容器的容器地址和业务机器的业务地址相同，避免了攻击者在业务子网内攻进蜜罐网络后，通过网络地址察觉到网络环境不对而退出蜜罐网络逃避蜜罐监控，返回攻击业务子网内其他真实业务的情况。让攻击者

15 拿下蜜罐容器后，误以为是成功拿下了业务机器的权限，从而达到迷惑攻击者的攻击，使其深陷蜜罐网络，进而保证业务机器的安全。

附图说明

为了更清楚地说明本公开或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见

20 地，下面描述中的附图是本公开的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是现有技术中构建的蜜罐网络示例图；

图 2 是根据本公开实施例的蜜罐网络运行方法的流程示意图；

25 图 3 是根据本公开实施例的蜜罐网络运行方法实现的网络示例图；

图 4 是根据本公开实施例的蜜罐网络运行装置的结构示意图；
图 5 是根据本公开实施例的电子设备的结构示意图。

具体实施方式

为使本公开实施例的目的、技术方案和优点更加清楚，下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚地描述，显然，所描述的实施例是本公开实施例一部分实施例，而不是全部的实施例。基于本公开实施例中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本公开实施例保护的范围。

10 图 1 示出了一种蜜罐网络。该网络中，业务子网占用的业务网段为 172.16.119.1 至 172.16.119.24（即 172.16.119.1/24），172.16.119.5、172.16.119.6 和 172.16.119.7 分别为该业务子网中不同业务机器的网络地址，172.16.119.4 为设置在业务子网中的蜜罐宿主机。通过该蜜罐宿主机构建蜜罐子网，该蜜罐子网占用的业务网段为 192.168.0.1
15 至 192.168.0.24（即 192.168.0.1/24），192.168.0.3、192.168.0.4、192.168.0.5 和 192.168.0.6 分别表示该蜜罐子网中不同蜜罐容器的网络地址。

当攻击者对业务子网进行攻击时，如图 1 中，攻击网络地址为 172.16.119.7 的业务机器时，则探针将该业务机器上的攻击流量转发到密网（即蜜罐子网）内，由蜜罐子网中地址为 192.168.0.4 的蜜罐容器提供虚拟服务。但是，攻击者对当前业务子网进行攻击拿下蜜罐容器内的服务后，会意识到当前网段的地址与之前业务不在同一个网段，且无法访问到之前的业务机器服务。攻击者很可能意识到自己处于蜜网环境内，从而停止对蜜罐机器的攻击，去攻击其他业务机器。

25 本公开提供一种新的蜜罐网络运行方法，使蜜罐容器和业务机器的网络地址相同。下面以蜜罐宿主机为执行主体，结合图 2-图 4 描述

本公开实施例提供的蜜罐网络运行方法。

在实施例中，如图 2 所示，蜜罐网络运行方法应用于蜜罐宿主机时，实现的过程如下：

步骤 201，获取业务机器的攻击流量。

5 本实施例中，攻击流量指的是攻击者访问业务机器的恶意访问流量。业务机器接收到攻击流量后，会通过预设的分流方法将攻击流量发送给该攻击流量发送给蜜罐宿主机，由蜜罐宿主机对攻击流量进行处理。

10 本实施例中，业务机器指的是运行真实业务服务的机器。每一个业务机器有对应的网络地址，用于实现多种服务。替代地，网络地址可以为互联网协议地址（Internet Protocol Address，简称 IP 地址）。蜜罐宿主机指的是用来创建蜜罐容器的主机，可以和真实的业务机器部署在同一个子网内。

15 步骤 202，将攻击流量转发至业务机器对应的蜜罐容器，其中，蜜罐容器的容器地址与业务机器的业务地址相同，业务地址为业务机器的网络地址，容器地址为蜜罐容器的网络地址。

20 本实施例中，蜜罐宿主机内预先创建了业务机器对应的蜜罐容器。蜜罐容器指的是易被攻击的万维网（World Wide Web，Web）服务或者安全外壳协议（Secure Shell Protocol，SSH）服务等，意图是让攻击者对其发起攻击，吸引火力，拖延攻击者对其他真实业务发起攻击的时间。蜜罐宿主机获取攻击流量之后，将攻击流量转发至业务机器对应的蜜罐容器中，由蜜罐容器提供攻击流量需要访问的服务。避免攻击者访问业务机器，保证业务机器的安全运行。

25 步骤 203，返回蜜罐容器生成的虚拟数据，其中，虚拟数据为攻击流量请求的数据，虚拟数据包括容器地址。

本实施例中，由蜜罐容器生成攻击流量需要的数据，即虚拟数据，

营造攻击者访问成功的假象。若攻击者发送的攻击流量请求了网络地址，则返回的虚拟数据中包括容器地址。而由于蜜罐容器和业务机器的网络地址相同，攻击者即使获得蜜罐容器的容器地址，也不会发现自身已经陷入了蜜罐环境，进而增强整个蜜罐环境的迷惑性，保证业务机器的安全。

在实施例中，蜜罐容器需要预先创建。替代地，获取业务机器的攻击流量之前，蜜罐宿主机获取业务机器的业务地址；根据业务地址，创建业务机器对应的蜜罐容器。

本实施例中，部署整个蜜罐网络时，蜜罐宿主机获取业务机器的业务地址，然后根据该业务地址，创建该业务机器对应的蜜罐容器。创建的该蜜罐容器拥有的蜜罐地址，与业务机器的业务地址一致。蜜罐容器创建完成后，蜜罐宿主机通过蜜罐容器实现对攻击流量的处理。

在实施例中，蜜罐宿主机和业务机器之间通过探针完成数据的传输。替代地，获取业务机器的业务地址，实现过程为：获取探针传输的业务地址，其中，探针位于业务机器，探针用于获取并转发业务机器的业务地址。获取业务机器的攻击流量，实现过程为：获取探针传输的攻击流量，其中，探针还用于转发访问业务机器的攻击流量。

本实施例中，蜜罐宿主机与业务机器上的探针连接，可以完成数据交互。而探针部署在真实的业务机器上，占用业务机器的端口。

探针是预先部署在业务机器上的模块，业务机器和蜜罐宿主机之间的数据传输通过探针来完成。一方面，探针可以将访问业务机器的攻击流量转发给蜜罐宿主机，即业务机器将攻击流量发送给探针，探针接收到该攻击流量后，再将该攻击流量发送给蜜罐宿主机，蜜罐宿主机完成对攻击流量的处理。另一方面，在创建蜜罐容器的阶段，探针从所在的业务机器上获取业务地址，然后将该业务地址传输给蜜罐宿主机，蜜罐宿主机获取探针传输的业务地址，以完成蜜罐容器的创

建。

本实施例中，蜜罐宿主机通过探针既可以获取攻击流量，还可以获取业务地址。先对于现有技术中探针只用于转发攻击流量，本实施例中探针实现了更多的功能，提高探针的利用率，减少资源浪费。

- 5 在实施例中，获取业务机器的业务地址之前，获取业务子网的业务网段，其中，业务网段包括业务子网占用的至少一个网络地址；根据业务网段，设置应用容器引擎，其中，应用容器引擎用于根据业务网段中的网络地址，创建网络地址对应的蜜罐容器。根据业务地址，创建业务机器对应的蜜罐容器，替代地，确定业务地址属于业务网段
- 10 后，调用应用容器引擎创建业务机器对应的蜜罐容器。

- 本实施例中，蜜罐宿主机部署在业务子网后，蜜罐宿主机可以执行获取网络接口配置信息的命令，例如 `ifconfig` 命令，获取该业务子网占用的业务网段，例如，该业务网段为 `172.16.119.1/24`。将该业务网段存储至蜜罐宿主机能够访问的存储器中。蜜罐宿主机获取该业务
- 15 网段后，根据该业务网段设置应用容器引擎（`docker`）。之后，蜜罐宿主机通过 `docker` 的方式来创建蜜罐网络。

- 替代地，蜜罐宿主机根据已经获得的业务网段设置 `docker` 启动方式。当蜜罐宿主机获得的业务地址属于已经存储的业务网段时，则自动启动 `docker`，动态创建蜜罐容器。设置 `docker` 启动方式的命令
- 20 可以采用以下语句：

```
docker network create --subnet=172.16.0.0/16 test;
```

其中，`172.16.0.0/16` 可以根据实际情况和需要替换为任意业务网段，例如，替换为 `172.16.119.1/24`。

- 通过上述过程即可简单实现每次部署蜜罐的时候，蜜网的网络环境都能自动去获取业务网段的信息，从而保持蜜罐网络的网段与业务网段一致。
- 25

- 在实施例中，为了增加蜜罐网络创建的灵活性和多样性，根据业务地址，创建业务机器对应的蜜罐容器之前，获取构建业务机器对应的蜜罐容器的蜜罐自定义指令，其中，蜜罐自定义指令包括蜜罐容器的执行方式和服务类型。根据业务地址，创建业务机器对应的蜜罐容器，替代地，根据业务地址，以蜜罐自定义指令中的执行方式和服务类型，创建业务机器对应的蜜罐容器，其中，蜜罐服务包括以服务类型建立的虚拟服务。而将攻击流量转发至业务机器对应的蜜罐容器之后，根据攻击流量，以执行方式执行虚拟服务。由该虚拟服务生成虚拟数据，然后将虚拟数据返回给攻击者。
- 10 本实施例中，蜜罐宿主机提供自定义服务。在建立蜜罐容器之间，蜜罐宿主机获取蜜罐自定义指令，该蜜罐自定义指令中包括蜜罐容器的执行方式和服务类型。建立蜜罐容器时，蜜罐自定义指令中的执行方式和服务类型，建立业务机器对应的蜜罐容器。例如，蜜罐自定义指令指示，以 shiro 命令的执行方式，执行蜜罐容器中的 Web 服务。当探针将业务机器的攻击流量转发至蜜罐宿主机后，蜜罐宿主机将攻击流量分发至该业务机器对应的蜜罐容器，按照自定义的 shiro 命令执行蜜罐容器内的 Web 服务。然后该 Web 服务生成虚拟数据，返回给攻击者，给攻击者营造访问成功的假象，为攻击溯源等反攻击处理过程提供更多时机。
- 15 在实施例中，业务机器的攻击流量需要通过端口，由探针转发给蜜罐宿主机。替代地，探针将业务地址传输给蜜罐宿主机之后，探针从自定义端口获取业务机器的攻击流量，其中，自定义端口与探针的连接关系，通过端口自定义指令设置完成；探针将攻击流量传输给蜜罐宿主机。
- 20 本实施例中，业务机器上转发攻击流量的端口，可以根据实际情况和/需要进行自定义。例如，自定义端口为业务机器的 8080 端口。
- 25

自定义端口提高了蜜罐网络运行过程中的灵活性。同时，由于指定了自定义端口，更容易通过该自定义端口监测针对业务子网的恶意攻击，以及更便于收集攻击流量，实现安全警报、攻击溯源等其他数据处理过程。

- 5 在实施例中，一个业务子网中包括至少一个业务机器，而蜜罐网络是针对整个业务子网的，也就是需要创建每一个业务机器对应的蜜罐容器。对于每一个业务机器，探针和业务机器是一一对应的，即每一个业务机器上部署对应的探针。各个探针均与蜜罐宿主机保持连接。则获取探针传输的业务地址，替代地，获取至少一个探针分别传输的
- 10 至少一个业务地址，其中，至少一个探针分别位于至少一个业务机器。根据业务地址，创建业务机器对应的蜜罐容器，替代地，根据至少一个业务地址，创建至少一个业务机器分别对应的蜜罐容器。获取探针传输的攻击流量，替代地，获取至少一个探针传输的、分别针对至少一个业务机器的攻击流量。将攻击流量转发至业务机器对应的蜜罐容器，替代地，将分别针对至少一个业务机器的攻击流量，分别转发至
- 15 至少一个业务机器分别对应的蜜罐容器。

- 本实施例中，当各个蜜罐容器生成各个业务机器对应的虚拟数据后，蜜罐宿主机将对应的虚拟数据，分别返回给访问各个业务机器的攻击者。整个蜜罐网络中的蜜罐容器，与业务子网中的业务机器是一
- 20 一对应的，实现了蜜罐网络和业务子网的一致性，提高蜜罐网络的迷惑性和仿真性，进一步保证业务子网的安全。

- 在实施例中，为了进一步保证蜜罐网络和业务子网一致，根据至少一个业务地址，创建至少一个业务机器分别对应的蜜罐容器之后，以预设时长为周期，将心跳信息发送给 N 个待监测探针，其中，以
- 25 预设时长为周期发送心跳信息给每一个待监测探针，其中，待监测探针指的是与蜜罐宿主机连接的探针，N 个待监测探针分别位于 N 个

业务机器，N 为大于或等于 1 的整数；获取 M 个待监测探针返回的反馈信息，确定 M 个待监测探针为活动探针，其中，活动探针为正常运行的探针，M 为大于或等于 1，且小于或等于 N 的整数；确定 M 个活动探针中的至少一个新增加探针，其中，新增加探针为未创建对应蜜罐容器的新增加业务机器对应的探针；分别获取每一个新增加探针传输的新增加业务地址；根据每一个新增加业务地址，分别建立每一个新增加业务机器对应的蜜罐容器。

本实施例中，蜜罐宿主机通过心跳信息，监测各个业务机器上的探针。当业务机器运行且探针正常时，探针在接收到心跳信息后，能够向蜜罐宿主机返回反馈信息，当业务机器没有运行，或者探针异常时，则不会返回反馈信息。

在蜜罐宿主机运行过程中，通过周期性的向各个探针发送心跳信息，能够监测业务子网的变化。若业务子网中新增加了业务机器，且该业务机器部署好探针后，蜜罐宿主机则可以通过新增加探针，获取新增加业务机器的新增加业务地址。此时，蜜罐宿主机则新建与新增加业务机器对应的蜜罐容器。

上述过程中，蜜罐宿主机不仅可以监测探针的存活状态，还可以实现蜜罐网络的动态调整，即当业务子网增加了业务机器时，即蜜罐网络中能够实时相应的增加蜜罐容器，保证了业务子网和蜜罐网络的一致性。攻击者在蜜罐网络中时，由于蜜罐容器与业务机器的网络地址一致，且还可以访问同一网段内的其他服务，极难察觉蜜网的存在，由于极大的提高了蜜网环境的仿真性，使得攻击者深陷蜜罐，为后期溯源提供更多数据支撑。

在实施例中，如图 3 所示的示例网络中，业务子网占用的业务网段为 172.16.119.1 至 172.16.119.24 (即 172.16.119.1/24)，172.16.119.7 和 172.16.119.8 分别为该业务子网中不同业务机器的 IP 地址。每一个

业务机器分别部署探针。172.16.119.6 为部署在业务子网中的蜜罐宿主机的 IP 地址。

- 蜜罐宿主机执行 `ifconfig` 命令，获得业务子网的业务网段为 172.16.119.1/24 之后，保存该业务网段。而后续建立的蜜罐容器的 IP 地址均属于该业务网段。蜜罐宿主机根据已获取的业务网段设置 `docker` 启动方式，动态创建相同网段的蜜罐网络，即图 3 中蜜罐子网的蜜网网段为相同的 172.16.119.1/24。攻击者对业务子网进行攻击时，进入蜜罐容器内的服务后，由于蜜罐网络网段与业务网段一致，不会意识到已经进入蜜罐网络。该方式极大的提高了蜜罐网络的迷惑性。
- 两个探针分别将 172.16.119.7 和 172.16.119.8 传输给蜜罐宿主机后，由蜜罐宿主机使用 `docker` 生成对应的两个蜜罐容器，两个蜜罐容器的 IP 地址分别为 172.16.119.7 和 172.16.119.8，与业务子网中两个业务机器的 IP 地址相同。

- 假设业务子网中新增加了业务机器，新增加业务机器的 IP 地址为 172.16.119.9，则蜜罐宿主机通过新增加探针获得 IP 地址 172.16.119.9 以后，使用 `docker` 再新生成 IP 地址 172.16.119.9 为蜜罐容器，实现动态调整蜜罐子网，实时保证蜜罐子网与业务子网的一致性，增强蜜罐子网的迷惑性。

- 本公开提供的蜜罐网络运行方法，获取业务机器的攻击流量之后，将攻击流量转发至业务机器对应的蜜罐容器，其中，蜜罐容器的容器地址与业务机器的业务地址相同，业务地址为业务机器的网络地址，容器地址为蜜罐容器的网络地址；最后返回蜜罐容器生成的虚拟数据，其中，虚拟数据为攻击流量请求的数据，虚拟数据包括容器地址。通过上述过程构建的蜜罐网络中，蜜罐容器的容器地址和业务机器的业务地址相同，避免了攻击者在业务子网内攻进蜜罐网络后，通过网络地址察觉到网络环境不对而退出蜜罐网络逃避蜜罐监控，返回攻击业

务子网内其他真实业务的情况。让攻击者拿下蜜罐容器后，误以为是成功拿下了业务机器的权限，从而达到迷惑攻击者的攻击，使其深陷蜜罐网络，进而保证业务机器的安全。

下面对本公开实施例提供的蜜罐网络运行的蜜罐宿主机装置进行描述，下文描述的蜜罐网络运行装置与上文描述的蜜罐网络运行方法可相互对应参照。如图 4 所示，蜜罐网络运行装置，包括：

获取模块 401，用于获取业务机器的攻击流量；

转发模块 402，用于将攻击流量转发至业务机器对应的蜜罐容器，其中，蜜罐容器的容器地址与业务机器的业务地址相同，业务地址为业务机器的网络地址，容器地址为蜜罐容器的网络地址；

返回模块 403，用于返回所述蜜罐容器生成的虚拟数据，其中，所述虚拟数据为所述攻击流量请求的数据，所述虚拟数据包括所述容器地址。

在实施例 1 中，蜜罐网络运行装置还包括预处理模块 404。

预处理模块 404，用于获取业务机器的攻击流量之前，获取业务机器的业务地址；根据业务地址，创建业务机器对应的蜜罐容器。

在实施例 2 中，预处理模块 404，具体用于获取探针传输的业务地址，其中，探针位于业务机器，探针用于获取并转发业务机器的业务地址。

获取模块 401，具体用于获取探针传输的攻击流量，其中，探针还用于转发访问业务机器的攻击流量。

在实施例 3 中，预处理模块 404，还用于获取业务机器的业务地址之前，获取业务子网的业务网段，其中，业务网段包括业务子网占用的至少一个网络地址；根据业务网段，设置应用容器引擎，其中，应用容器引擎用于根据业务网段中的网络地址，创建网络地址对应的蜜罐容器。

预处理模块 404，具体用于确定业务地址属于业务网段后，调用应用容器引擎创建业务机器对应的蜜罐容器。

在实施例中，预处理模块 404，还用于根据业务地址，创建业务机器对应的蜜罐容器之前，获取构建业务机器对应的蜜罐容器的蜜罐自定义指令，其中，蜜罐自定义指令包括蜜罐容器的执行方式和服务类型。

预处理模块 404，具体用于根据业务地址，以蜜罐自定义指令中的执行方式和服务类型，创建业务机器对应的蜜罐容器，其中，蜜罐服务包括以服务类型建立的虚拟服务。

10 蜜罐网络运行装置还包括执行模块 405。执行模块 405 用于将攻击流量转发至业务机器对应的蜜罐容器之后，根据攻击流量，以执行方式执行虚拟服务。

在实施例中，预处理模块 404，具体用于获取至少一个探针分别传输的至少一个业务地址，其中，至少一个探针分别位于至少一个业务机器；根据至少一个业务地址，创建至少一个业务机器分别对应的蜜罐容器。

获取模块 401，具体用于获取至少一个探针传输的、分别针对至少一个业务机器的攻击流量。

20 转发模块 402，具体用于将分别针对至少一个业务机器的攻击流量，分别转发至至少一个业务机器分别对应的蜜罐容器。

在实施例中，蜜罐网络运行装置还包括实时处理模块 406。实时处理模块 406，用于根据至少一个业务地址，创建至少一个业务机器分别对应的蜜罐容器之后，以预设时长为周期，将心跳信息发送给 N 个待监测探针，其中，以预设时长为周期发送心跳信息给每一个待监测探针，其中，待监测探针指的是与蜜罐宿主机连接的探针，N 个待监测探针分别位于 N 个业务机器，N 为大于或等于 1 的整数；获取

M个待监测探针返回的反馈信息,确定M个待监测探针为活动探针,其中,活动探针为正常运行的探针,M为大于或等于1,且小于或等于N的整数;确定M个活动探针中的至少一个新增加探针,其中,新增加探针为未创建对应蜜罐容器的新增加业务机器对应的探针;

5 分别获取每一个新增加探针传输的新增加业务地址;根据每一个新增加业务地址,分别建立每一个新增加业务机器对应的蜜罐容器。

图5示例了一种电子设备的实体结构示意图,如图5所示,该电子设备可以包括:处理器(processor)501、通信接口(Communications Interface)502、存储器(memory)503和通信总线504,其中,处理器501,
10 通信接口502,存储器503通过通信总线504完成相互间的通信。处理器501可以调用存储器503中的逻辑指令,以执行蜜罐网络运行方法,该方法包括:获取业务机器的攻击流量;将攻击流量转发至业务机器对应的蜜罐容器,其中,蜜罐容器的容器地址与业务机器的业务地址相同,业务地址为业务机器的网络地址,容器地址为蜜罐容器的
15 网络地址;返回蜜罐容器生成的虚拟数据,其中,虚拟数据为攻击流量请求的数据,虚拟数据包括容器地址。

此外,上述的存储器503中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用,可以存储在计算机可读取存储介质中。基于这样的理解,本公开实施例的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来,该计算机软件产品存储在存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本公开各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM, Read-Only
20 Memory)、随机存取存储器(RAM, Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

另一方面，本公开还提供一种计算机程序产品，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算机程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，计算机能够执行上述各方法所提供的蜜罐网络运行方法，该方法包括：获取业务机器的攻击流量；将攻击流量转发至业务机器对应的蜜罐容器，其中，蜜罐容器的容器地址与业务机器的业务地址相同，业务地址为业务机器的网络地址，容器地址为蜜罐容器的网络地址；返回蜜罐容器生成的虚拟数据，其中，虚拟数据为攻击流量请求的数据，虚拟数据包括容器地址。

又一方面，本公开还提供一种非暂态计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现以执行上述各提供的蜜罐网络运行方法，该方法包括：获取业务机器的攻击流量；将攻击流量转发至业务机器对应的蜜罐容器，其中，蜜罐容器的容器地址与业务机器的业务地址相同，业务地址为业务机器的网络地址，容器地址为蜜罐容器的网络地址；返回蜜罐容器生成的虚拟数据，其中，虚拟数据为攻击流量请求的数据，虚拟数据包括容器地址。

以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性的劳动的情况下，即可以理解并实施。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软

件产品可以存储在计算机可读存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行各个实施例或者实施例的某些部分所述的方法。

- 5 最后应说明的是：以上实施例仅用以说明本公开的技术方案，而非对其限制；尽管参照前述实施例对本公开进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本公开各实施例技术方案的精神和范围。
- 10

权 利 要 求 书

1、一种蜜罐网络运行方法，包括：

获取业务机器的攻击流量；

5 将所述攻击流量转发至所述业务机器对应的蜜罐容器，其中，所述蜜罐容器的容器地址与所述业务机器的业务地址相同，所述业务地址为所述业务机器的网络地址，所述容器地址为所述蜜罐容器的网络地址；

返回所述蜜罐容器生成的虚拟数据，其中，所述虚拟数据为所述攻击流量请求的数据，所述虚拟数据包括所述容器地址。

10 2、根据权利要求 1 所述的蜜罐网络运行方法，其中，所述获取业务机器的攻击流量之前，还包括：

获取所述业务机器的所述业务地址；

根据所述业务地址，创建所述业务机器对应的所述蜜罐容器。

15 3、根据权利要求 2 所述的蜜罐网络运行方法，其中，所述获取所述业务机器的所述业务地址，包括：

获取探针传输的所述业务地址，其中，所述探针位于所述业务机器，所述探针用于获取并转发所述业务机器的所述业务地址；

所述获取业务机器的攻击流量，包括：

20 获取探针传输的所述攻击流量，其中，所述探针还用于转发访问所述业务机器的所述攻击流量。

4、根据权利要求 2 所述的蜜罐网络运行方法，其中，所述获取所述业务机器的所述业务地址之前，还包括：

获取业务子网的业务网段，其中，所述业务网段包括所述业务子网占用的至少一个所述网络地址；

25 根据所述业务网段，设置应用容器引擎，其中，所述应用容器引擎用于根据所述业务网段中的所述网络地址，创建所述网络地址对应

的所述蜜罐容器；

所述根据所述业务地址，创建所述业务机器对应的蜜罐容器，包括：

确定所述业务地址属于所述业务网段后，调用所述应用容器引擎

5 创建所述业务机器对应的所述蜜罐容器。

5、根据权利要求 2 所述的蜜罐网络运行方法，其中，所述根据所述业务地址，创建所述业务机器对应的所述蜜罐容器之前，包括：

获取构建所述业务机器对应的蜜罐容器的蜜罐自定义指令，其中，所述蜜罐自定义指令包括所述蜜罐容器的执行方式和服务类型；

10 所述根据所述业务地址，创建所述业务机器对应的所述蜜罐容器，包括：

根据所述业务地址，以所述蜜罐自定义指令中的所述执行方式和所述服务类型，创建所述业务机器对应的所述蜜罐容器，其中，所述蜜罐服务包括以所述服务类型建立的虚拟服务；

15 所述将所述攻击流量转发至所述业务机器对应的蜜罐容器之后，还包括：

根据所述攻击流量，以所述执行方式执行所述虚拟服务。

6、根据权利要求 3 所述的蜜罐网络运行方法，其中，所述获取探针传输的所述业务地址，包括：

20 获取至少一个探针分别传输的至少一个所述业务地址，其中，至少一个所述探针分别位于至少一个所述业务机器；

所述根据所述业务地址，创建所述业务机器对应的所述蜜罐容器，包括：

25 根据至少一个所述业务地址，创建至少一个所述业务机器分别对应的所述蜜罐容器；

所述获取探针传输的所述攻击流量，包括：

获取至少一个所述探针传输的、分别针对至少一个所述业务机器的所述攻击流量；

所述将所述攻击流量转发至所述业务机器对应的蜜罐容器，包括：

将分别针对至少一个所述业务机器的所述攻击流量，分别转发至

5 至少一个所述业务机器分别对应的所述蜜罐容器。

7、根据权利要求 6 所述的蜜罐网络运行方法，其中，所述根据至少一个所述业务地址，创建至少一个所述业务机器分别对应的所述蜜罐容器之后，还包括：

以预设时长为周期，将心跳信息发送给 N 个待监测探针，其中，

10 以预设时长为周期发送心跳信息给每一个待监测探针，其中，所述待监测探针指的是与所述蜜罐宿主机连接的探针，所述 N 个待监测探针分别位于 N 个所述业务机器，N 为大于或等于 1 的整数；

获取 M 个所述待监测探针返回的反馈信息，确定所述 M 个所述待监测探针为活动探针，其中，所述活动探针为正常运行的探针，M

15 为大于或等于 1，且小于或等于 N 的整数；

确定所述 M 个所述活动探针中的至少一个新增加探针，其中，所述新增加探针为未创建对应蜜罐容器的新增加业务机器对应的探针；

分别获取每一个所述新增加探针传输的新增加业务地址；

20 根据每一个所述新增加业务地址，分别建立每一个所述新增加业务机器对应的所述蜜罐容器。

8、一种蜜罐网络运行装置，包括：

获取模块，用于获取业务机器的攻击流量；

25 转发模块，用于将所述攻击流量转发至所述业务机器对应的蜜罐容器，其中，所述蜜罐容器的容器地址与所述业务机器的业务地址相同，所述业务地址为所述业务机器的网络地址，所述容器地址为所述

蜜罐容器的网络地址；

返回模块，用于返回所述蜜罐容器生成的虚拟数据，其中，所述虚拟数据为所述攻击流量请求的数据，所述虚拟数据包括所述容器地址。

5 9、一种电子设备，包括：

处理器；以及

存储器，存储了可在处理器上运行的计算机程序，其中，所述处理器执行所述程序时执行如权利要求 1 至 7 任一项所述蜜罐网络运行方法。

10 10、一种非暂态计算机可读存储介质，其上存储有计算机程序，其中，所述计算机程序被处理器执行时执行如权利要求 1 至 7 任一项所述蜜罐网络运行方法。