(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 104917757 A
(43)申请公布日 2015.09.16

(21)申请号 201510233838.X

(22)申请日 2015.05.08

(71)申请人 中国科学院信息工程研究所
地址 100093 北京市海淀区闵庄路甲89号

(72)发明人 闫兆腾 黄伟武 芦翔 朱红松 孙利民

(74)专利代理机构 北京轻创知识产权代理有限公司 11212
代理人 杨立

(51)Int.Cl.
H04L 29/06(2006.01)
G06F 21/32(2013.01)

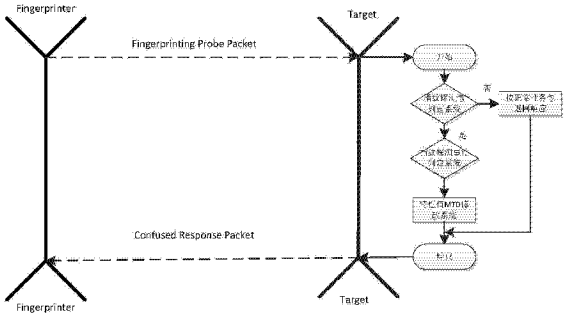
权利要求书3页 说明书8页 附图2页

(54)发明名称

一种事件触发式的MTD防护系统及方法

(57)摘要

本发明涉及一种事件触发式的MTD防护系统及方法。本发明通过对操作系统主动指纹识别方法和探测包的分析，制定探测事件集，设计一种事件触发式的MTD隐藏操作系统特征的防护思想。实现被防护目标(Target)每次收到指纹探测方(Fingerprinter)的探测数据包时，自动更改该探测项对应特性，使探测方收集到的指纹特征是错误的信息，从而使被欺骗或混淆为其他设备类型，最终使一些重要基础设备得到一个有效的抗远程指纹识别的防护机制。



CN 104917757 A

1.一种事件触发式的MTD防护系统，其特征在于，包括指纹探测包判定系统、指纹探测事件判定系统和特性值MTD修改系统；

所述指纹探测包判定系统，其用于收到来自客户端发来的请求数据包时，进行对数据包是属于正常业务数据包还是属于探测系统特性的指纹探测包等类型的判别，如果判定为正常系统业务连接请求数据包，则不做任何处理直接响应而不触发防护机制；如果判定为旨在获取当前系统特性及对应特性值的探测包，则立刻触发防护机制，确保系统特性信息的不外泄；

所述指纹探测事件判定系统，其用于收集、存储和判断指纹探测的事件，在判定收到了探测数据包时，首先在指纹探测事件集中比对，是否已在当前事件集中，如果已存在则按当前事件的处理方法对应执行；如果未存在，则将探测包想要探测特性的值进行随机化修改，然后将这种类型的探测行为定义一条新增事件记录并存储；

所述特性值MTD修改系统，其用于在判定为指纹探测行为后，利用MTD思想，对被探测部分特性的值在一定范围内执行随机化或布尔变换，然后将更改后的特性值封装成响应数据包返回给指纹探测方。

2.根据权利要求1所述一种事件触发式的MTD防护系统，其特征在于，所述指纹探测包判定系统包括数据包解析模块、数据包类型判别模块、数据包目标端口判别模块、数据包内容判别模块和数据包特征判别模块；

所述数据包解析模块是用于解析收到的请求数据包，拆开包的封装来查看数据包的包头、目的地址、目的端口、数据包类型、数据包内容等，为后续判别的模块提供源数据；

所述数据包类型判别模块、数据包目标端口判别模块和数据包内容判别模块之间相互配合完成数据包是正常业务包还是指纹探测数据包的判定，从而决定是否触发指纹探测事件集和MTD修改系统；

所述数据包特征判别模块是结合数据包类型判别模块、数据包目标端口判别模块和数据包内容判别模块以及数据包特征判别模块等提供的源数据，判断当前指纹探测是属于哪种探测类型。

3.根据权利要求1所述一种事件触发式的MTD防护系统，其特征在于，所述指纹探测事件判定系统包括探测类型判别模块、探测事件数据库和探测事件分类模块；

所述探测类型判别模块，用于对探测数据包按协议类型进行分类，将探测数据包传递给指纹探测事件判定系统；

所述探测事件数据库，事先存储好的IP、TCP、UDP和ICMP不同协议探测的事件特征集；

所述探测事件分类模块，用于将探测类型判别模块判断的数据与探测事件数据库相匹配，如果与其中一项匹配成功，则执行该事件对应的MTD修改系统的执行步骤，如果不能与其中一项匹配成功，则将当前探测类型按事件数据库的格式新增一条事件规则，最后将本次探测类型所要探测的特性传递给下一步的特征值的MTD修改系统。

4.根据权利要求1所述一种事件触发式的MTD防护系统，其特征在于，所述特性值MTD修改系统包括对应特性的值更改模块；所述特征值的MTD修改系统，是将当前探测包所要探测的特性值进行欺骗性修改，如果是一个数值，则在指定范围内执行随机化；如果是一个布尔值，则将当前的布尔值进行非运算。最后将修改后的结果按响应数据包格式封装，返回

给指纹探测方。

5. 一种事件触发式的 MTD 防护方法，其特征在于，包括如下步骤：

利用指纹探测包判定系统收到来自客户端发来的请求数据包时，进行对数据包是属于正常业务数据包还是属于探测系统特性的指纹探测包等类型的判别，如果判定为正常系统业务连接请求数据包，则不做任何处理直接响应而不触发防护机制；如果判定为旨在获取当前系统特性及对应特性值的探测包，则立刻触发防护机制，确保系统特性信息的不外泄；

利用指纹探测事件判定系统收集、存储和判断指纹探测的事件，在判定收到了探测数据包时，首先在指纹探测事件集中比对，是否已在当前事件集中，如果已存在则按当前事件的处理方法对应执行；如果未存在，则将探测包想要探测特性的值进行随机化修改，然后将这种类型的探测行为定义一条新增事件记录并存储；

利用特性值 MTD 修改系统在判定为指纹探测行为后，利用 MTD 思想，对被探测部分特性的值在一定范围内执行随机化或布尔变换，然后将更改后的特性值封装成响应数据包返回给指纹探测方。

6. 根据权利要求 5 所述一种事件触发式的 MTD 防护方法，其特征在于，判定数据包是正常业务数据包还是恶意探测包的判定过程如下：

步骤 1.1：数据包解析模块模块对数据包进行解封装；

步骤 1.2：数据包类型判别模块对当前数据包的协议类型进行判别，如果是 ICMP 协议，直接将当前数据包定义为探测包，执行步骤 1.5 并将当前探测包类型标签定义为 ICMP；如果是 IP 协议，执行步骤 1.4 的数据包内容判别模块；如果是 TCP 或 UDP 协议，则执行步骤 1.3 数据包目标端口判别模块；

步骤 1.3：数据包目标端口判别模块对数据包中目标端口是否开放进行判别，如果是开放，执行步骤 1.4 数据包内容判别模块；如果是关闭的，则将当前数据包定义为探测包，执行步骤 1.5，并根据协议类型将当前探测包类型标签定义为 TCP 或 UDP；

步骤 1.4：数据包内容判别模块对数据包中的数据部分进行判别，如果数据为空，则将当前数据包定义为探测包，执行步骤 1.5；如果数据包不为空，则认为当前数据包为正常的业务数据包并正常返回响应数据包；

步骤 1.5：探测类型判别模块对探测数据包按协议类型进行分类，类型标签主要分为 ICMP、IP、TCP 和 UDP 四种，然后探测数据包传递给指纹探测事件判定系统进行后续操作。

7. 根据权利要求 5 所述一种事件触发式的 MTD 防护方法，其特征在于，判定当前探测数据包属于哪种探测事件的过程如下：

步骤 2.1：根据探测数据包的探测类型 tag 与探测事件数据库进行匹配，如果是已知的探测事件，则执行步骤 2.2，如果是未知的探测事件，则将当前探测类型按事件数据库的格式新增一条事件规则，最后将本次探测类型所要探测的特性传递给下一步的特征值的 MTD 修改系统；

步骤 2.2：根据步骤 2.1 中的探测类型 tag 与探测事件数据库匹配判定当前探测事件是当前数据库中包含已知的探测事件，执行一步 switch 匹配，根据不同类型的 tag 执行相对应的 MTD 特性修改步骤。

8. 根据权利要求 5 所述一种事件触发式的 MTD 防护方法，其特征在于，所述各种探测事

件对应想探测的特性值，实现迷惑性的过程为：

步骤 3.1：探测事件对应探测的特性值是否为布尔型进行判别；

步骤 3.2：如果是布尔型，则执行一步非运算，将当前的特性值变成相反的，从而实现对探测结果的欺骗，如果不是布尔型，再执行步骤 3.3；

步骤 3.3：由步骤 3.2 判定当前探测的特征值不是布尔型，而是一个数值，则执行随机化算法，将当前的特性值在一个不影响系统正常的范围内，进行随机化变换，使探测结果每次都不具有规律，实现对探测结果的混淆；

步骤 3.4：将修改后的特性值进行封装成数据包返回给探测方。

9. 根据权利要求 5 所述一种事件触发式的 MTD 防护方法，其特征在于，所述探测数据包同时包含一种协议下几个特性值的探测，通过将每个特性值的探测定义为一个事件，使每个探测事件的判定和 MTD 欺骗修改与其他事件独立开。

一种事件触发式的 MTD 防护系统及方法

技术领域

[0001] 本发明涉及国家重要基础设备隐藏防护领域，尤其涉及一种事件触发式的 MTD 防护系统及方法。

背景技术

[0002] 在当前环境下，信息技术系统是建立在相对静态的配置中运行。例如，地址、名称、软件栈、网络和各种配置参数在较长的时间段内保持相对静态。这种静态的方法使意图对系统进行恶意漏洞利用 (exploit) 的攻击者可以有充足的时间搜索、探测和识别目标系统的版本和配置等信息，其中最具代表性的就是操作系统指纹探测和识别 (Operating System Fingerprinting Detection)，即通过对网络上的主机进行主动的 (active) 或被动的 (passive) 探测数据包的特性 (feature) 差异信息收集来确定所使用的操作系统，通常被攻击者作为攻击前信息采集中最重要的一步。

[0003] MTD(Moving Target Defense) 思想是基于控制跨多个系统维度的变化，增加系统的不确定性和复杂性，从而减少攻击者的攻击表面 (attack surface) 和增加攻击成本而提出的一个新概念。自 2011 年 MTD 被提出来后，已逐渐发展成系统防护领域的研究热点，并被美国白宫确定为未来发展的四大网络空间安全防护战略技术之一。

[0004] 作为一种重要的安全防范系统，近年来，MTD 思想不仅在软件系统防范漏洞扫描和服务及版本防泄漏方面获得了应用，而且也逐渐在对抗远程操作系统指纹探测和识别上获得了大规模的推广。

[0005] MTD 思想在防范安全防范操作系统指纹识别系统方面的研究，在 2011 年主要集中在 IP 地址配置在一定周期内的随机化，使指纹探测方无法对目标主机的 IP 变换的时间窗口内完成信息采集和探测。在 2013 年的研究开始在远程操作系统指纹识别领域的 MTD 上，对 TCP 协议栈特性值进行周期性修改和防护。但是，由于周期性的 MTD 防护本身存在的安全缺陷以及安全隐患目前，如果探测方利用每个周期内只探测一个特性的方法，利用多个周期汇总每个特性的探测结果，就可以使 MTD 防护系统的安全机制和性能大大降低。另外考虑到指纹探测方如果采用分布式探测和信息采集的话，使 MTD 面对的攻击表面更加难以防范，使对抗指纹探测的情况更加复杂，周期性 MTD 防护的缺陷也更加凸显。

发明内容

[0006] 本发明所要解决的技术问题是针对现有技术的不足，提供一种事件触发式的 MTD 防护系统及方法。

[0007] 本发明解决上述技术问题的技术方案如下：一种事件触发式的 MTD 防护系统，包括指纹探测包判定系统、指纹探测事件判定系统和特性值 MTD 修改系统；

[0008] 所述指纹探测包判定系统，其用于收到来自客户端发来的请求数据包时，进行对数据包是属于正常业务数据包还是属于探测系统特性的指纹探测包等类型的判别，如果判定为正常系统业务连接请求数据包，则不做任何处理直接响应而不触发防护机制；如果判

定为旨在获取当前系统特性及对应特性值的探测包，则立刻触发防护机制，确保系统特性信息的不外泄；

[0009] 所述指纹探测事件判定系统，其用于收集、存储和判断指纹探测的事件，在判定收到了探测数据包时，首先在指纹探测事件集中比对，是否已在当前事件集中，如果已存在则按当前事件的处理方法对应执行；如果未存在，则将探测包想要探测特性的值进行随机化修改，然后将这种类型的探测行为定义一条新增事件记录并存储；

[0010] 所述特性值 MTD 修改系统，其用于在判定为指纹探测行为后，利用 MTD 思想，对被探测部分特性的值在一定范围内执行随机化或布尔变换，然后将更改后的特性值封装成响应数据包返回给指纹探测方。

[0011] 本发明的有益效果是：本发明的有益效果是：本发明采用事件触发式 MTD 对抗操作系统指纹识别机制，通过对操作系统主动指纹识别方法和探测包的分析，制定探测事件集，设计一种事件触发式的 MTD（隐藏操作系统特征的防护思想。从而实现被防护目标 (Target) 每次收到指纹探测方 (Fingerprinter) 的探测数据包时，自动更改该探测项对应特性，使探测方收集到的指纹特征是错误的信息，从而使被欺骗或混淆为其他设备类型，最终使一些重要基础设备得到一个有效的抗远程指纹识别的防护机制。

[0012] 本发明解决上述技术问题的另一技术方案如下：一种事件触发式的 MTD 防护方法，包括如下步骤：

[0013] 利用指纹探测包判定系统收到来自客户端发来的请求数据包时，进行对数据包是属于正常业务数据包还是属于探测系统特性的指纹探测包等类型的判别，如果判定为正常系统业务连接请求数据包，则不做任何处理直接响应而不触发防护机制；如果判定为旨在获取当前系统特性及对应特性值的探测包，则立刻触发防护机制，确保系统特性信息的不外泄；

[0014] 利用指纹探测事件判定系统收集、存储和判断指纹探测的事件，在判定收到了探测数据包时，首先在指纹探测事件集中比对，是否已在当前事件集中，如果已存在则按当前事件的处理方法对应执行；如果未存在，则将探测包想要探测特性的值进行随机化修改，然后将这种类型的探测行为定义一条新增事件记录并存储；

[0015] 利用特性值 MTD 修改系统在判定为指纹探测行为后，利用 MTD 思想，对被探测部分特性的值在一定范围内执行随机化或布尔变换，然后将更改后的特性值封装成响应数据包返回给指纹探测方。

附图说明

[0016] 图 1 为本发明一种事件触发式的 MTD 防护系统示意图；

[0017] 图 2 为本发明所述指纹探测包判定系统示意图；

[0018] 图 3 为本发明所述指纹探测事件判定系统示意图；

[0019] 图 4 为本发明所述特性值 MTD 修改系统系统示意图；

[0020] 图 5 为本发明所述一种事件触发式的 MTD 防护方法流程图；

[0021] 图 6 为本发明所述指纹探测包判定系统程序流程图；

[0022] 图 7 为本发明所述指纹探测事件判定程序流程图；

[0023] 图 8 为本发明所述特性值 MTD 修改程序流程图。

具体实施方式

[0024] 以下结合附图对本发明的原理和特征进行描述，所举实例只用于解释本发明，并非用于限定本发明的范围。

[0025] 发明涉及一种事件触发式对抗远程操作系统指纹识别(Remote Operating System Fingerprinting)的MTD(Moving Target Defense)防护系统。通过对操作系统主动指纹识别方法和探测包的分析，制定探测事件集，设计一种事件触发式的MTD隐藏操作系统特征的防护思想。实现被防护目标(Target)每次收到指纹探测方(Fingerprinter)的探测数据包时，自动更改该探测项对应特性，使探测方收集到的指纹特征是错误的信息，从而使被欺骗或混淆为其他设备类型，最终使一些重要基础设备得到一个有效的抗远程指纹识别的防护机制。

[0026] 如图1所示，一种事件触发式的MTD防护系统，包括指纹探测主机(fingerprinter)、被探测目标主机(target)和指纹探测MTD防护系统，其中指纹探测MTD防护系统部署在被探测目标主机上，包括指纹探测包判定系统、指纹探测事件判定系统和特性值MTD修改系统。

[0027] 所述指纹探测包判定系统，其用于收到来自客户端发来的请求数据包时，进行对数据包是属于正常业务数据包还是属于探测系统特性的指纹探测包等类型的判别。如果判定为正常系统业务连接请求数据包，则不做任何处理直接响应而不触发防护机制；如果判定为旨在获取当前系统特性及对应特性值的探测包，则立刻触发防护机制，确保系统特性信息的不外泄；

[0028] 所述指纹探测事件判定系统，其用于收集、存储和判断指纹探测的事件，在判定收到了探测数据包时，首先在指纹探测事件集中比对，是否已在当前事件集中，如果已存在则按当前事件的处理方法对应执行；如果未存在，则将探测包想要探测特性的值进行随机化修改，然后将这种类型的探测行为定义一条新增事件记录并存储；

[0029] 所述特性值MTD修改系统，其用于在判定为指纹探测行为后，利用MTD思想，对被探测部分特性的值在一定范围内执行随机化或布尔变换，然后将更改后的特性值封装成响应数据包返回给指纹探测方。

[0030] 在特性值MTD修改系统在对特性值为布尔型时，不仅可以采用当前的非运算来更改特性值，还可以采用非、异或等运算的随机化，使探测方更能对布尔型特性值指纹识别被防护的操作系统。所述探测事件集如表1。

[0031] 表1

[0032]

协议类型	特性集		示例
ICMP	identifier	16bit	数值
	sequence number	16bit	数值
TCP	sequence number	32bit	数值
	ACK number	32bit	数值
	urgent pointer	16bit	数值
	fragment	16bit	数值
	window size	16bit	数值
	flags	6bit	U A P R S F (布尔型)
	checksum	16bit	数值
UDP	length	16bit	数值

[0033]

IP	IP TTL value	8bit	数值
	IP ID	16bit	数值
	type of service	8bit	数值
	fragment	16bit	布尔型

[0034] 本发明核心在于当前数据包是否属于探测包及属于哪种类型的探测。

[0035] 如图 2 所示，所述指纹探测包判定系统包括数据包解析模块、数据包类型判别模块、数据包目标端口判别模块、数据包内容判别模块和数据包特征判别模块；所述数据包解析模块是用于解析收到的请求数据包，拆开包的封装来查看数据包的包头、目的地址、目的端口、数据包类型、数据包内容等，为后续判别的模块提供源数据；所述数据包类型判别模块、数据包目标端口判别模块和数据包内容判别模块之间相互配合完成数据包是正常业务包还是指纹探测数据包的判定，从而决定是否触发指纹探测事件集和 MTD 修改系统；所述数据包特征判别模块是结合数据包类型判别模块、数据包目标端口判别模块和数据包内容判别模块以及数据包特征判别模块等提供的源数据，判断当前指纹探测是属于哪种探测类型。

[0036] 如图 3 所示，所述指纹探测事件判定系统包括探测类型判别模块、探测事件数据库和探测事件分类模块；所述探测类型判别模块，对探测数据包按协议类型进行分类，类型标签 (tag) 主要分为 ICMP、IP、TCP 和 UDP 四种，然后探测数据包传递给指纹探测事件判定系统进行后续操作。所述探测事件数据库，事先存储好的 IP、TCP、UDP 和 ICMP 不同协议探测的事件特征集；所述探测事件分类模块，用于将探测类型判别模块判断的数据与探测事件数据库相匹配，如果与其中一项匹配成功，则执行该事件对应的 MTD 修改系统的执行步骤，如果不能与其中一项匹配成功，则将当前探测类型按事件数据库的格式新增一条事件规则，最后将本次探测类型所要探测的特性传递给下一步的特征值的 MTD 修改系统。

[0037] 如图 4 所示，所述特性值 MTD 修改系统包括对应特性的值更改模块；所述特征值的 MTD 修改系统，是将当前探测包所要探测的特性值进行欺骗性修改，如果是一个数值，则在指定范围内执行随机化；如果是一个布尔值，则将当前的布尔值进行非运算。最后将修改后的结果按响应数据包格式封装，返回给指纹探测方。

[0038] 如图 5 所示，一种事件触发式的 MTD 防护方法，包括如下步骤：

[0039] 利用指纹探测包判定系统收到来自客户端发来的请求数据包时，进行对数据包是属于正常业务数据包还是属于探测系统特性的指纹探测包等类型的判别，如果判定为正常系统业务连接请求数据包，则不做任何处理直接响应而不触发防护机制；如果判定为旨在获取当前系统特性及对应特性值的探测包，则立刻触发防护机制，确保系统特性信息的不外泄；

[0040] 利用指纹探测事件判定系统收集、存储和判断指纹探测的事件，在判定收到了探测数据包时，首先在指纹探测事件集中比对，是否已在当前事件集中，如果已存在则按当前事件的处理方法对应执行；如果未存在，则将探测包想要探测特性的值进行随机化修改，然后将这种类型的探测行为定义一条新增事件记录并存储；

[0041] 利用特性值 MTD 修改系统在判定为指纹探测行为后，利用 MTD 思想，对被探测部分特性的值在一定范围内执行随机化或布尔变换，然后将更改后的特性值封装成响应数据包返回给指纹探测方。

[0042] 如图 6 所示，所述数据包解析模块、数据包类型判别模块、数据包目标端口判别模块和数据包内容判别模块之间相互配合完成数据包是正常业务数据包还是恶意探测包的判定过程如下：

[0043] 步骤 1.1：数据包解析模块模块对数据包进行解封装；

[0044] 步骤 1.2：数据包类型判别模块对当前数据包是属于 ICMP、TCP、UDP、IP 中哪种协议类型数据包进行判别。如果是 ICMP 协议，直接将当前数据包定义为探测包，执行步骤 1.5 并将当前探测包类型标签 (tag) 定义为 ICMP；如果是 IP 协议，执行步骤 1.4 的数据包内容判别模块；如果是 TCP 或 UDP 协议，则执行步骤 1.3 数据包目标端口判别模块；

[0045] 步骤 1.3：数据包目标端口判别模块对数据包中目标端口是否开放进行判别，如果是开放，执行步骤 1.4 数据包内容判别模块；如果是关闭的，则将当前数据包定义为探测包，执行步骤 1.5，并根据协议类型将当前探测包类型标签 (tag) 定义为 TCP 或 UDP；

[0046] 步骤 1.4：数据包内容判别模块对数据包中的数据部分进行判别，如果数据为空，则将当前数据包定义为探测包，执行步骤 1.5；如果数据包不为空，则认为当前数据包为正常的业务数据包并正常返回响应数据包；

[0047] 步骤 1.5：探测类型判别模块对探测数据包按协议类型进行分类，类型标签 (tag) 主要分为 ICMP、IP、TCP 和 UDP 四种，然后探测数据包传递给指纹探测事件判定系统进行后续操作。

[0048] 如图 7 所示，所述探测事件数据库，是已经事先存储好的 IP、TCP、UDP 和 ICMP 等不同协议探测的事件特征集。所述探测事件分类模块，用于将探测类型判别模块判断的数据与探测事件数据库相匹配，如果与其中一项匹配成功，则执行该事件对应的 MTD 修改系统的执行步骤，如果不能与其中一项匹配成功，则将当前探测类型按事件数据库的格式新增一条事件规则，最后将本次探测类型所要探测的特性传递给下一步的特征值的 MTD 修改系统；

[0049] 所述一种指纹探测事件判定系统，其特征在于，所述探测事件分类模块与探测事件数据库对当前探测数据包属于哪种探测事件进行判定的过程如下：

[0050] 步骤 2.1：根据探测数据包的探测类型 tag 与探测事件数据库进行匹配，如果是已

知的探测事件，则执行步骤 2.2，如果是未知的探测事件，则将当前探测类型按事件数据库的格式新增一条事件规则，最后将本次探测类型所要探测的特性传递给下一步的特征值的 MTD 修改系统；

[0051] 步骤 2.2：根据步骤 2.1 中的探测类型 tag 与探测事件数据库匹配判定当前探测事件是当前数据库中包含已知的探测事件，执行一步 switch 匹配，根据不同类型的 tag 执行相对应的 MTD 特性修改步骤；例如 TCP 探测事件，则执行将当前 TCP 中产生特性值的初始序列号 (ISN, initial sequence number) 等执行 MTD 特性修改。

[0052] 如图 8 所示，所述特征值的 MTD 修改系统，是将当前探测包所要探测的特性值进行欺骗性修改，如果是一个数值，则在指定范围内执行随机化；如果是一个布尔值，则将当前的布尔值进行非运算。最后将修改后的结果按响应数据包格式封装，返回给指纹探测方。

[0053] 所述一种特性值的 MTD 修改系统，其特征在于，所述各种探测事件对应想探测的特性值，实现迷惑性修改的过程为：

[0054] 步骤 3.1：探测事件对应探测的特性值是否为布尔型进行判别；

[0055] 步骤 3.2：如果是布尔型，则执行一步非运算，将当前的特性值变成相反的，从而实现对探测结果的欺骗，如果不是布尔型，在执行步骤 3.3；

[0056] 步骤 3.3：由步骤 3.2 判定当前探测的特征值不是布尔型，而是一个数值，则执行随机化算法，将当前的特性值在一个不影响系统正常的范围内，进行随机化变换，使探测结果每次都不具有规律，实现对探测结果的混淆；

[0057] 步骤 3.4：将修改后的特性值进行封装成数据包返回给探测方。

[0058] 所述一种事件触发式的 MTD 防护系统，其特征在于，所述探测数据包可能同时包含一种协议下几个特性值的探测，而本发明的要旨即是通过将每个特性值的探测定义为一个事件，使每个探测事件的判定和 MTD 欺骗修改与其他事件独立开，从而使以 Nmap 为代表的综合多种探测事件结果来检测当前操作系统正确指纹的可能性大大降低。

[0059] 如图 1 所示，利用本发明所述事件触发式的 MTD 防护系统，可实现被防护主机能够欺骗和混淆攻击方的操作系统指纹探测和识别。根据被防护主机与其他主机建立连接的通信过程，将所有的防护过程总体上分为三个场景：

[0060] 即场景 1（正常业务数据通信 Client 相关协议的请求 TCP 连接 Target，在经过 MTD 防护系统检测确认当前数据包不是探测包，按正常响应包返回给 Client）；

[0061] 场景 2（指纹探测方 Fingerprinter 发送 TCP 协议中数据为空的 SYN 探测包给目标主机 Target，在经过 MTD 防护系统检测确认当前数据包是探测包，触发指纹识别 MTD 系统，将相应探测的特性值进行修改后，封装返回给 Fingerprinter）；

[0062] 场景 3（指纹探测方 Fingerprinter 发送 UDP 协议中探测包，其中目标端口为 Target 主机上关闭的端口，在经过 MTD 防护系统检测确认当前数据包是探测包，触发指纹识别 MTD 系统，将相应探测事件探测的端口进行修改为开放状态，封装 UDP 相应包返回给 Fingerprinter）。

[0063] 场景 1，正常 Client 请求与目标主机建立通信而未触发 MTD 防护机制，具体步骤如下：

[0064] 1）Client 首先向目标主机 Target 发送 TCP SYN 包；

[0065] 2）Target 通过事件触发式的 MTD 防护系统中的数据包解析模块对数据包进行解

封装；

[0066] 3) 数据包类型判别模块识别当前数据包为 TCP 协议类型；

[0067] 4) 数据包内容判别模块识别当前 TCP 数据包内容不为空，非探测包，从而不必触发探测事件检测和防护机制；

[0068] 5) 最后将 TCP SYN 包按正常业务返回包类型返回 ACK+SYN 包。

[0069] 场景 2，Target 对抗 Fingerprinter 的 TCP SYN 探测包，具体步骤如下：

[0070] 1)Fingprinter 向目标主机 Target 发送 TCP SYN 探测包，其中数据部分 data 为空；

[0071] 2)Target 通过事件触发式的 MTD 防护系统中的数据包解析模块对数据包进行解封装；

[0072] 3) 数据包类型判别模块识别当前数据包为 TCP 协议类型；

[0073] 4) 数据包目标端口判定模块识别当前数据包的目标端口是开放的；

[0074] 5) 数据包内容判别模块识别当前 TCP 数据包内容为空，进而判定是探测包，触发了探测事件检测和防护机制；

[0075] 6) 数据包特征判别模块将当前探测包的类型 tag 定义为 TCP SYN 探测，并将参数传递给指纹探测事件判定系统；

[0076] 7) 指纹探测事件判定系统根据探测包的 tag 中的 TCP SYN 探测，与探测事件数据库中匹配得知当前探测事件是当前已知的探测事件；

[0077] 8) 指纹探测事件判定系统经过 switch 匹配，将当前 TCP SYN 探测事件对应探测的特性值包括 ISN(initial sequence number,32bit)、ACK number(32bit)、urgent pointer(16bit)、window size(16bit)、flags 中 SYN(1bit)、checksum(16bit)，参数传递给特性值的 MTD 修改系统；

[0078] 9) 特性值的 MTD 修改系统对 ISN、ACK number、urgent pointer、window size、flags 中 SYN(1bit)、checksum 每个特性进行是否为布尔值进行判别，判别只有 flags 中 SYN(1bit) 为布尔值，其他的特性都是数值；

[0079] 10) 特性值的 MTD 修改系统对当前的 flags 中的 SYN 值进行非运算，对其他特性的值执行随机化计算；

[0080] 11) 特性值的 MTD 修改系统对修改后的特性值进行封装成 ACK+SYN 返回给 Fingerprinter。

[0081] 场景 3，Target 对抗 Fingerprinter 的 UDP 对关闭目标端口的探测包，具体包括以下操作：

[0082] 1)Fingprinter 向目标主机 Target 发送 UDP 探测包，其中目标端口是 Target 关闭端口；

[0083] 2)Target 通过事件触发式的 MTD 防护系统中的数据包解析模块对数据包进行解封装；

[0084] 3) 数据包类型判别模块识别当前数据包为 UDP 协议类型；

[0085] 4) 数据包目标端口判定模块识别当前数据包的目标端口是关闭的，将当前数据包定义为探测包；

[0086] 5) 数据包特征判别模块将当前探测包的类型 tag 定义为 UDP 探测，并将参数传递

给指纹探测事件判定系统；

[0087] 6)指纹探测事件判定系统经过switch匹配，将当前TCP SYN探测事件对应探测的特性值包括了IPID(identification,16bit)和length(16bit)，参数传递给特性值的MTD修改系统；

[0088] 7)特性值的MTD修改系统对IP ID和length这两个特性进行是否为布尔值进行判别，特性都是数值；

[0089] 8)特性值的MTD修改系统对当前特性的值执行随机化计算；

[0090] 9)特性值的MTD修改系统对修改后的特性值进行封装成UDP响应包返回给Fingerprinter。

[0091] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

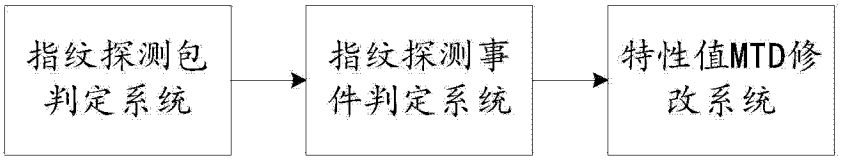

指纹探测包判定系统
指纹探测事件判定系统
特性值MTD修改系统

图 1

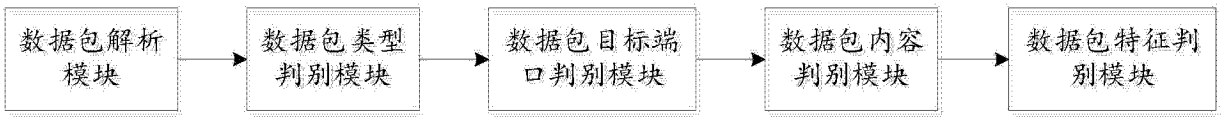

数据包解析模块
数据包类型判别模块
数据包目标端口判别模块
数据包内容判别模块
数据包特征判别模块

图 2


探测类型判别模块
探测事件数据库
探测事件分类模块

图 3


特性值MTD修改系统
对应特性的值更改模块

图 4

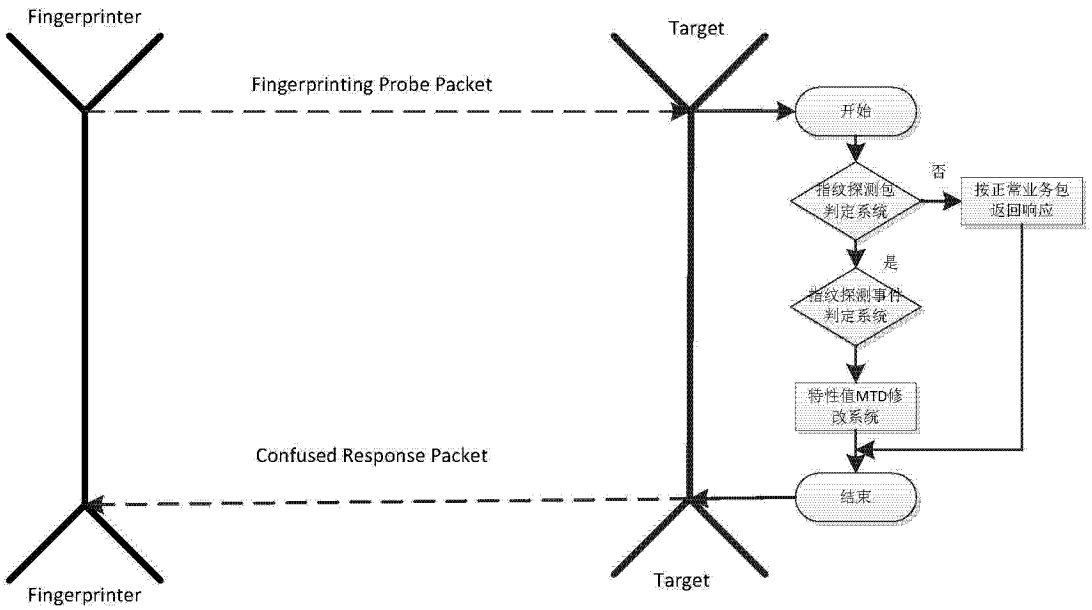

Fingerprinter
Target
Fingerprinting Probe Packet
开始
指纹探测包判定系统
否
按正常业务包返回响应
是
指纹探测事件判定系统
特性值MTD修改系统
Confused Response Packet
结束
Fingerprinter
Target

图 5

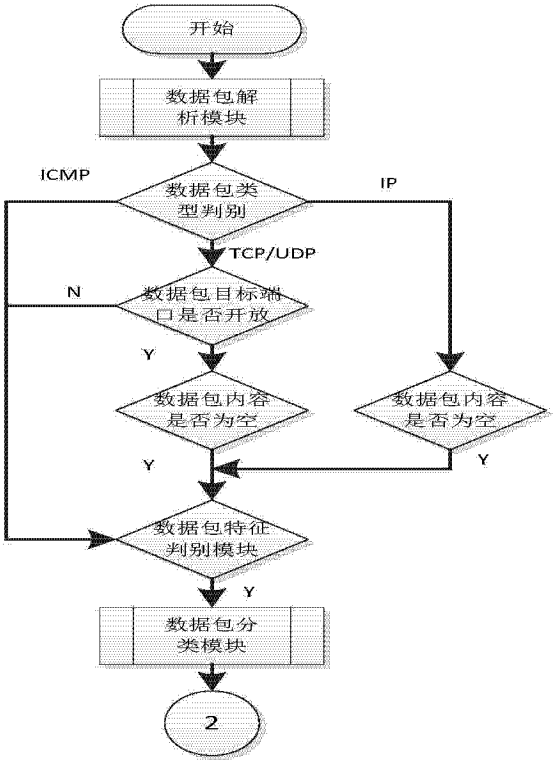

开始
数据包解析模块
ICMP
数据包类型判别
IP
TCP/UDP
N
数据包目标端口是否开放
Y
数据包内容是否为空
数据包内容是否为空
Y
Y
数据包特征判别模块
Y
数据包分类模块
2

图 6

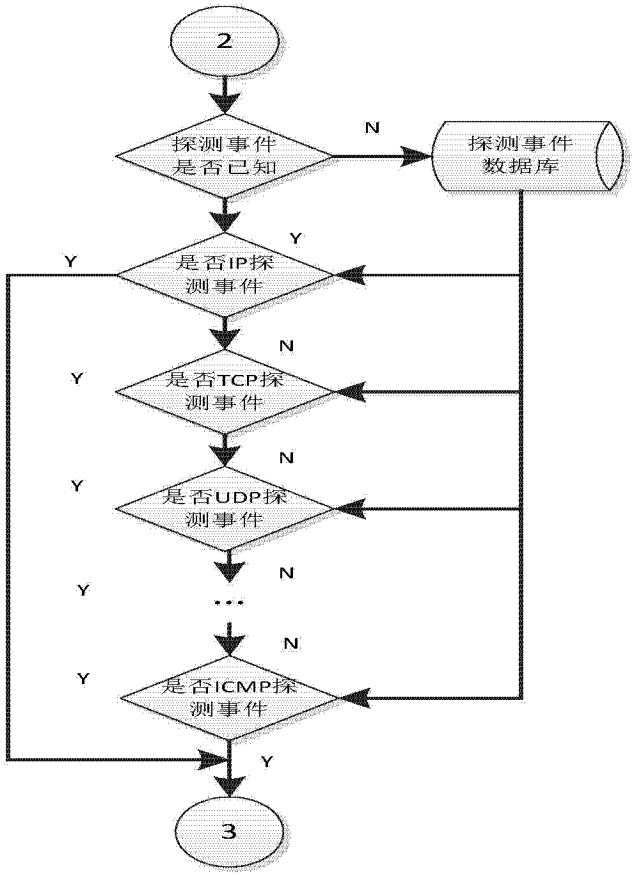

2
探测事件是否已知
N
探测事件数据库
Y
Y
是否IP探测事件
Y
N
是否TCP探测事件
Y
N
是否UDP探测事件
Y
N
...
Y
N
是否ICMP探测事件
Y
3

图 7

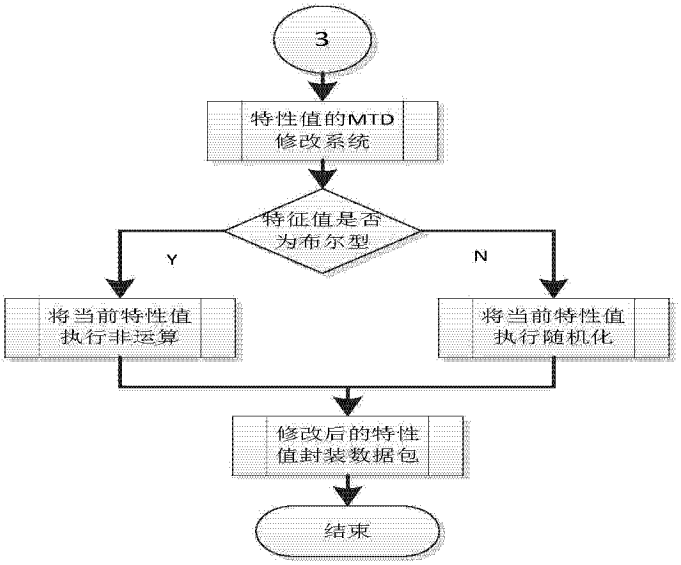

3
特性值的MTD修改系统
特征值是否为布尔型
Y
N
将当前特性值执行非运算
将当前特性值执行随机化
修改后的特性值封装数据包
结束

图 8