(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1643876 B
(45)授权公告日 2010.09.29

(21)申请号 03807319.6

(22)申请日 2003.03.28

(30)优先权数据
60/319,159 2002.03.29 US

(85)PCT申请进入国家阶段日
2004.09.28

(86)PCT申请的申请数据
PCT/US2003/009665 2003.03.28

(87)PCT申请的公布数据
WO2003/084181 EN 2003.10.09

(73)专利权人 思科技术公司
地址 美国加利福尼亚州

(72)发明人 克雷格·H·罗兰

(74)专利代理机构 北京东方亿思知识产权代理有限责任公司 11258
代理人 王怡

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/26(2006.01)
G06F 1/00(2006.01)

(56)对比文件
WO 01/84270 A2,2001.11.08, 说明书第6页第1段-第15页第4段、附图1-8.
CN 1310393 A,2001.08.29, 全文.
WO 02/19077 A2,2002.03.07, 全文.
EP 0985995 A1,2000.03.15, 全文.

审查员 张迎新

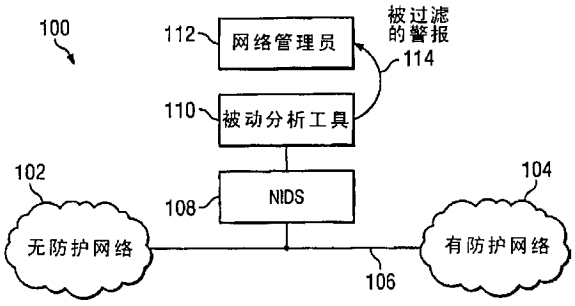
权利要求书 4 页 说明书 5 页 附图 3 页

(54)发明名称

用于降低网络入侵检测系统的误报率的方法和系统

(57)摘要

根据本发明的一个实施例,提出了一种用于降低网络入侵检测系统的误报率的方法,包括:接收表明可能发生了网络入侵的警报;识别警报的特征,至少包括攻击类型和目标地址;询问与目标地址相关联的目标主机以获得操作系统指纹;从目标主机接收包括操作系统类型的操作系统指纹;将攻击类型与操作系统类型进行比较;并且基于所述比较,表明目标主机是否可能受到攻击。



CN 1643876 B

1. 一种用于降低网络入侵检测系统的误报率的方法，包括：

接收表明可能发生了网络入侵的警报；

识别所述警报的特征，至少包括攻击类型和目标地址；

访问存储位置；

确定在所述存储位置中，是否存在所述目标地址的操作系统指纹；

响应于在所述存储位置中不存在所述目标地址的所述操作系统指纹，询问与所述目标地址相关联的目标主机以获得操作系统指纹；

从所述目标主机接收包括操作系统类型的所述操作系统指纹；

将所述攻击类型与所述操作系统类型进行比较；以及

基于所述比较，表明所述目标主机是否可能受到所述攻击。

2. 如权利要求 1 所述的方法，还包括在一段时期内，在所述存储位置中存储所述目标主机的所述操作系统指纹。

3. 如权利要求 1 所述的方法，还包括：

如果在所述存储位置中，存在所述目标主机的所述操作系统指纹，那么：

确定所述目标地址的缓存条目时间是否有效；并且

如果所述缓存条目时间有效，那么继续所述方法的所述比较步骤；否则

如果所述缓存条目时间无效，那么继续所述方法的所述询问步骤。

4. 如权利要求 1 所述的方法，还包括：

监视动态配置协议服务器；

检测出现了新目标主机的租用发生事件；

访问存储位置；

确定在所述存储位置是否已经存在所述新目标主机的操作系统指纹；以及

如果所述新目标主机的所述操作系统指纹不存在，那么：

询问所述新目标主机以获得所述操作系统指纹；

从所述新目标主机接收所述操作系统指纹；并且

在一段时期内，在所述存储位置中存储所述新目标主机的所述操作系统指纹；并且

如果所述新目标主机的所述操作系统指纹存在，那么：

从所述存储位置删除所述新目标主机的已经存在的操作系统指纹；

询问所述新目标主机以获得新操作系统指纹；

从所述新目标主机接收所述新操作系统指纹；并且

在一段时期内，在所述存储位置中存储所述新目标主机的所述新操作系统指纹。

5. 如权利要求 1 所述的方法，还包括：

监视动态配置协议服务器；

检测出现了现有目标主机的租用到期事件；

访问存储位置；

确定在所述存储位置是否已经存在所述现有目标主机的操作系统指纹；以及

如果所述现有目标主机的所述操作系统指纹不存在，那么忽略所述租用到期事件；并且

如果所述现有目标主机的所述操作系统指纹存在，那么从所述存储位置删除所述现有

目标主机的所述已经存在的操作系统指纹。

6. 如权利要求 1 所述的方法，还包括：

在接收到所述警报后，确定所述警报的格式是否有效；并且

如果所述格式无效，那么忽略所述警报；否则

如果所述格式有效，那么继续所述方法的所述识别步骤。

7. 一种用于降低网络入侵检测系统的误报率的方法，包括：

接收表明可能发生了网络入侵的警报；

识别所述警报的特征，至少包括攻击类型、源地址、目标地址、警报严重性和警报描述；

访问存储位置；

确定在所述存储位置是否已经存在与所述目标地址相关联的目标主机的操作系统指纹；

如果所述目标主机的操作系统指纹不存在，那么：

询问所述目标主机以获得所述操作系统指纹；

从所述目标主机接收包括操作系统类型的所述操作系统指纹；

将所述攻击类型与所述操作系统类型进行比较；并且

基于所述比较，表明所述目标主机是否易于受到所述攻击；

如果所述目标主机的所述操作系统指纹存在，那么：

确定所述目标地址的缓存条目时间是否有效；并且

如果所述缓存条目时间无效，那么：

询问所述目标主机以获得所述操作系统指纹；

从所述目标主机接收包括操作系统类型的所述操作系统指纹；

将所述攻击类型与所述操作系统类型进行比较；并且

基于所述比较，表明所述目标主机是否可能受到所述攻击；如果所述缓存条目时间有效，那么：

将所述攻击类型与所述操作系统类型进行比较；并且

基于所述比较，表明所述目标主机是否可能受到所述攻击。

8. 如权利要求 7 所述的方法，还包括在一段时期内，在所述存储位置存储所述目标主机的所述操作系统指纹。

9. 如权利要求 7 所述的方法，还包括：

监视动态配置协议服务器；

检测出现了新目标主机的租用发生事件；

访问所述存储位置；

确定在所述存储位置是否已经存在所述新目标主机的操作系统指纹；以及

如果所述新目标主机的所述操作系统指纹不存在，那么：

询问所述新目标主机以获得所述操作系统指纹；

从所述新目标主机接收所述操作系统指纹；并且

在一段时期内，在所述存储位置存储所述新目标主机的所述操作系统指纹；并且

如果所述新目标主机的所述操作系统指纹存在，那么：

从所述存储位置删除所述新目标主机的所述已经存在的操作系统指纹；

询问所述新目标主机以获得新操作系统指纹；

从所述新目标主机接收所述新操作系统指纹；并且

在一段时期内，在所述存储位置中存储所述新目标主机的所述新操作系统指纹。

10. 如权利要求 7 所述的方法，还包括：

监视动态配置协议服务器；

检测出现了现有目标主机的租用到期事件；

访问所述存储位置；

确定在所述存储位置是否已经存在所述现有目标主机的操作系统指纹；以及

如果所述现有目标主机的所述操作系统指纹不存在，那么忽略所述租用到期事件；并且

如果所述现有目标主机的所述操作系统指纹存在，那么从所述存储位置删除所述现有目标主机的所述已经存在的操作系统指纹。

11. 一种用于降低网络入侵检测系统的误报率的系统，包括：

用于接收表明可能发生了网络入侵的警报的装置；

用于识别至少包括攻击类型和目标地址的所述警报的特征的装置；

用于访问存储位置的装置；

用于确定在所述存储位置中是否存在所述目标地址的操作系统指纹的装置；

用于响应于在所述存储位置中不存在所述目标地址的所述操作系统指纹来询问与所述目标地址相关联的目标主机以获得操作系统指纹的装置；

用于从所述目标主机接收包括操作系统类型的所述操作系统指纹的装置；

用于将所述攻击类型与所述操作系统类型进行比较的装置；以及

用于基于所述比较，表明所述目标主机是否可能受到所述攻击的装置。

12. 如权利要求 11 所述的系统，还包括用于在一段时期内，在所述存储位置中存储所述目标主机的所述操作系统指纹的装置。

13. 如权利要求 11 所述的系统，还包括：

当在所述存储位置中存在所述目标主机的所述操作系统指纹时，用于确定所述目标地址的缓存条目时间是否有效的装置。

14. 如权利要求 11 所述的系统，还包括：

用于监视动态配置协议服务器的装置；

用于检测出现了新目标主机的租用发生事件的装置；

用于访问存储位置的装置；

用于确定在所述存储位置是否已经存在所述新目标主机的操作系统指纹的装置；并且

如果所述新目标主机的所述操作系统指纹不存在，那么还包括：

用于询问所述新目标主机以获得所述操作系统指纹的装置；

用于从所述新目标主机接收所述操作系统指纹的装置；以及

用于在一段时期内，在所述存储位置中存储所述新目标主机的所述操作系统指纹的装置；并且

如果所述新目标主机的所述操作系统指纹存在，那么还包括：

用于从所述存储位置删除所述新目标主机的已经存在的操作系统指纹的装置；

用于询问所述新目标主机以获得新操作系统指纹的装置；

用于从所述新目标主机接收所述新操作系统指纹的装置；以及

用于在一段时期内，在所述存储位置中存储所述新目标主机的所述新操作系统指纹的装置。

15. 如权利要求 11 所述的系统，还包括：

用于监视动态配置协议服务器的装置；

用于检测出现了现有目标主机的租用到期事件的装置；

用于访问存储位置的装置；

用于确定在所述存储位置是否已经存在所述现有目标主机的操作系统指纹的装置；并且

如果所述现有目标主机的所述操作系统指纹不存在，那么还包括用于忽略所述租用到期事件的装置；并且

如果所述现有目标主机的所述操作系统指纹存在，那么还包括用于从所述存储位置删除所述现有目标主机的已经存在的操作系统指纹的装置。

用于降低网络入侵检测系统的误报率的方法和系统

技术领域

[0001] 本发明一般地涉及入侵检测，更具体地说，涉及用于降低网络入侵检测系统的误报率的方法和系统。

背景技术

[0002] 网络入侵检测系统（“NIDS”）一般被设计用来实时监视网络活动以发现可疑的或已知的恶意活动，并将这些发现报告给适当的人员。通过密切监视所有的活动，NIDS 能够比较迅速地发出计算机入侵警报，并且给管理员时间以防卫或遏制入侵，或者让 NIDS 自动对攻击作出反应并阻止攻击。在安全工业中，NIDS 可以是被动型的流量观察器，也可以是实时作出反应以阻止攻击的主动型的网络部件。

[0003] 因为 NIDS 是被动型的网络流量观察器，所以它们经常缺乏关于攻击主机和防护主机的某些知识，这使得它不能确定攻击是否成功。与正在偷听两个陌生人之间对话的偷听者非常相似，NIDS 常常缺乏关于攻击的上下文的知识，因此会对可能是非敌意的或无关的网络活动“发出警报”。

[0004] 一些系统试图通过对它们所监视的网络建立静态映象来解决这个问题。这种知识的建立通常要通过扫描网络上的所有系统，并且将结果保存在数据库中以用于以后的检索。这种系统对于大多数的网络来说是不够用的，因为网络设备的拓扑、类型和位置是不断变化的，而且这种系统需要管理员维护静态的数据库。此外，持续扫描和保持网络数据库的更新的压力很大，可能经常会导致网络服务变慢或停止工作。

发明内容

[0005] 根据本发明的一个实施例，提出了一种用于降低网络入侵检测系统的误报率的方法，包括：接收表明可能发生了网络入侵的警报；识别警报的特征，至少包括攻击类型和目标地址；询问与目标地址相关联的目标主机以获得操作系统指纹；从目标主机接收包括操作系统类型的操作系统指纹；将攻击类型与操作系统类型进行比较；并且基于所述比较，表明目标主机是否可能受到攻击。

[0006] 本发明的一些实施例提供许多技术优点。其它的实施例可能实现一些或全部这些优点，也可能一个也实现不了。例如，根据一个实施例，网络入侵检测系统（“NIDS”）的误报率被极大地降低或消除，而这降低了对监视 NIDS 以对每个警报作出反应的人员的需求。即使不需要关于整个有防护网络的知识，也可获得较低的误报率。因为不再需要网络的知识，因此可以动态地向网络增加主机。根据另一个实施例，对网络的严重的攻击被升级，而且损失很大的入侵被补救。

[0007] 本领域的技术人员可以很容易地通过下面的附图、具体实施方式和权利要求书来发现其它的优点。

附图说明

[0008] 现在将参考下面的与附图相结合的说明，以获得对本发明及其优点的更加全面的理解，在附图中，相似的标号代表相似的部分，并且：

[0009] 图 1 的示意图根据本发明的一个实施例，示出了使用被动分析工具来降低网络入侵检测系统的误报率的系统；

[0010] 图 2 的方框图根据本发明的一个实施例，示出了图 1 中的被动分析工具的各种功能部件；

[0011] 图 3 的流程图根据本发明的一个实施例，示出了用于降低网络入侵检测系统的误报率的方法；并且

[0012] 图 4 的流程图根据本发明的一个实施例，示出了可以与图 3 的方法结合起来使用的方法。

具体实施方式

[0013] 参考所附图 1 到图 4 可以最好地理解本发明的实施例，相似的标号被用于各图中相似的和相应的部分。

[0014] 图 1 的示意图根据本发明的一个实施例，示出了使用被动分析工具 110 来降低网络入侵检测系统（“NIDS”）108 的误报率的系统 100。在所示实施例中，NIDS 108 耦合到链路 106，链路 106 可通信地耦合了无防护网络 102 和有防护网络 104。系统 100 还包括使用被动分析工具 110 的网络管理员 112，如下面所详细描述的那样。

[0015] 无防护网络 102 可以是有防护网络 104 外部的任何合适的网络。无防护网络 102 的一个例子是因特网。有防护网络 104 可以是任何合适的网络，例如局域网、广域网、虚拟专用网络或任何其它的希望其安全性不受无防护网络 102 影响的网络。链路 106 将无防护网络 102 耦合到有防护网络 104，并且其可以是任何合适的通信链路或信道。在一个实施例中，链路 106 能够在无防护网络 102 和有防护网络 104 之间以“包”传输数据；但是，通信链路 106 也可以以其它合适的形式来传输数据。

[0016] 在一个实施例中，NIDS 108 是任何合适的基于网络的入侵检测系统，其能够分析在通信链路 106 上传输的数据包，以检测对有防护网络 104 的任何潜在攻击。NIDS 108 可以是硬件、固件和 / 或软件的任何合适的组合。一般地，NIDS 108 包括一个或更多个传感器，它们能够监视具有任何合适的数据链路协议的任何合适类型的网络。在具体的实施例中，与 NIDS 108 相关联的传感器能够检查使用任何合适协议（例如 TCP（“传输控制协议”）、UDP（“用户数据报协议”）和 ICMP（“网间控制报文协议”））的 IP（“因特网协议”）网络上的数据包。在检测到对有防护网络 104 的可能的攻击后，NIDS 108 能够产生表明可能发生了对有防护网络 104 的攻击的警报，并可以立刻阻止该攻击。然后，该警报被传输到被动分析工具 110 以进行如下所述的分析。

[0017] 根据本发明的一个实施例的教导，被动分析工具 110 接收来自 NIDS108 的警报，使用与该警报关联的信息，确定是真的发生了攻击还是收到了错误的警报。被动分析工具 110 显著地降低了网络环境中的网络入侵检测系统（如 NIDS 108）的误报率，并且减少了对监视这些系统以对每个警报作出反应的人员（例如网络管理员 112）的需求。被动分析工具 110 的细节将在下面结合图 2 到 4 而被更详细地说明。虽然被动分析工具 110 在图 1 中被

示为与NIDS 108相分离，但是它也可以与NIDS 108集成在一起，这样就不需要分立的硬件了。在任何情况下，NIDS 108和被动分析工具110都协同工作，以根据检测到的攻击的严重性和精确性来分析、降低或升级警报。本发明的一个技术优点是可以消除目标为错误的操作系统、供应商、应用或网络硬件的警报。

[0018] 网络管理员112可以是使用被动分析工具110来监视对有防护网络104的潜在攻击，并在适当情况下对其进行反应的任何合适的人员。网络管理员112一般具有驻留在他的或她的计算机上的被动分析工具110，以接收来自被动分析工具的被过滤了的警报，如标号114所指。

[0019] 图2的方框图根据本发明的一个实施例，示出了被动分析工具110的各种功能部件。本发明考虑到了部件的数量比图2所示更多、更少，或与图2所示部件不同的情况。在图示的实施例中，被动分析工具110包括警报输入层202、警报解释层204、目标缓存查找206、操作系统（“OS”）取指纹（fingerprinting）机制208、端口取指纹机制210和警报输出层212。在结合图3到4对被动分析工具110的功能进行更详细的描述之前，现在描述这些部件中每个部件的一般功能。

[0020] 警报输入层202一般负责接受来自NIDS 108的警报，并将其传递到其它系统部件进行分析。在一个实施例中，警报输入层202接受来自NIDS 108的警报，并确定该警报格式是否有效。如果该警报格式无效，那么该警报被忽略。如果该警报格式有效，那么该警报被发送到警报解释层204。警报输入层202被优选地设计为不依赖于NIDS供应商，这样它就可以不作修改地同时接受来自多个NIDS源的警报。

[0021] 一般地，警报解释层204从警报输入层202接收警报并对该警报执行分析。在一个实施例中，警报解释层204确定该警报是否来自于被支持的NIDS供应商。如果该警报不是来自于被支持的NIDS供应商，那么一个警告被产生，并且该警报被忽略。如果该警报是来自于被支持的NIDS供应商，那么警报解释层204负责确定该NIDS供应商的警报类型、被攻击的相关操作系统类型（例如Microsoft Windows、Sun Solaris、Linux、UNIX等）、源地址、目标网络地址、警报严重性、警报描述以及任何其它合适的与该警报相关联的参数。被动分析工具110使用该信息中的一些信息来测试该警报的真假，下面会结合图3和4进行更详细的描述。

[0022] 目标缓存查找206表明查找由被动分析工具110执行，以确定是否针对于该警报所表明的特定攻击而检查过目标主机。可以在任何合适的存储位置（例如在本地状态表或数据库中）执行查找。

[0023] OS取指纹机制208对目标主机执行被动分析，以确定该目标主机的操作系统。简单地说，在一个实施例中，被动分析工具110向目标主机发送其头部具有协议标志、选项以及其它合适的信息的特定组合的因特网协议（“IP”）包，以确认操作系统供应商和版本号。操作系统取指纹在工业上是公知的，因此这里不再详述。这种类型的OS取指纹的一个优点是，它不需要除远程网络连接之外的对目标主机的内部访问。OS取指纹机制208可以在几秒钟的执行时间内建立操作系统类型，并将此信息存储在合适的存储位置，以用于以后的检索和使用。

[0024] 端口取指纹机制210的功能是在主机被动态增加和删除时，识别存储在合适的存储位置的目标端口地址。端口取指纹机制210与OS取指纹机制208协同工作，以确定例如

目标主机上的被攻击端口是否是活动的。这使得被动分析工具 110 可以迅速地确定攻击能否成功。例如，通过检查目标主机，看其端口 80 是否本来处于活动状态，可以证明对目标主机的 TCP 端口 80 的攻击是否已经失败。

[0025] 警报输出层 212 负责从被动分析工具 110 取得分析数据并将警报升级或降级。换句话说，警报输出层 212 的作用是报告有效的警报，即，特定目标主机可能受到攻击。有效警报可以以任何合适的方式被报告，所述方式例如是图形用户界面、日志文件、数据库中的存储或任何其它合适的输出。

[0026] 根据本发明的一个实施例，下面结合图 3 和图 4 进一步描述被动分析工具 110 的功能细节。

[0027] 图 3 的流程图根据本发明的一个实施例，示出了用于降低网络入侵检测系统的误报率的示例性方法。该示例性方法从步骤 300 开始，在此处被动分析工具 110 从 NIDS 108 接收到警报。在步骤 302，被动分析工具 110 从该警报识别目标地址。然后，在步骤 304，被动分析工具 110 访问系统缓存，以确定是否已经对目标主机进行过关于该特定攻击类型的检查。

[0028] 相应地，在判断步骤 306，确定是否已经在系统缓存中找到目标地址。如果目标地址被找到了，那么在判断步骤 308，确定缓存条目的时间是否仍然有效。换句话说，如果特定的目标主机在最近一段时间内由于特定类型的攻击而被检查过，那么该信息就被暂时存储在系统缓存中。尽管可以使用任何合适的时间段来存储该信息，但是在一个实施例中，该信息的存储时间不多于 1 小时。如果缓存条目时间仍然有效，那么继续执行所述方法到步骤 310，在此处被动分析工具 110 接收目标主机的 OS 指纹。

[0029] 回到判断步骤 306 和 308，如果在系统缓存中没有找到该目标地址，或在系统缓存中找到的特定目标地址的缓存条目时间是无效的，那么被动分析工具 110 使用任何合适的 OS 取指纹技术来获得目标主机的操作系统指纹，如步骤 312 所示。然后，在步骤 314，操作系统指纹被存储在系统缓存中。然后继续执行所述方法到步骤 310，在此处被动分析工具 110 接收目标主机的 OS 指纹。

[0030] 在步骤 316，被动分析工具 110 比较攻击类型和目标主机的操作系统类型。在判断步骤 318，确定目标主机的操作系统类型和攻击类型是否匹配。如果匹配，那么在步骤 320，报告被确认的警报。如果不匹配，那么表明是错误警报，如步骤 322 所示。例如，如果攻击类型是针对 Windows 系统的而操作系统指纹显示为 Windows 主机，那么该警报被确认。但是，如果攻击类型是针对 Windows 系统的而操作系统指纹显示为 UNIX 主机，那么这就表明是错误警报。然后，图 3 所示的示例性方法结束。

[0031] 虽然图 3 所示的方法是参考将操作系统类型与攻击类型进行比较的被动分析工具 110 来进行说明的，但是也可以将操作系统的其它合适的特征与攻击类型的相关特征进行比较，以确定警报的真假。

[0032] 因此，被动分析工具 110 是智能过滤技术，其过滤掉潜在的错误警报而不需要关于整个有防护网络 104 的知识。从所部署的 NIDS（例如 NIDS108）接收警报输入，并进行分析以确定该攻击是真的还是收到了假警报。即使不要求在有防护网络 104 的每个计算设备上都安装代理，也能够实现上述功能。

[0033] 图 4 的流程图根据本发明的一个实施例，示出了可以与图 3 的示例性方法相结合使用的示例性方法。图 4 中的示例性方法从步骤 400 开始，在此处被动分析工具 110 监视

动态主机配置协议（“DHCP”）服务器。本发明考虑到了由被动分析工具 110 监视的任何合适的动态配置协议服务器。在步骤 402，被动分析工具 110 检测到租用行为。在判断步骤 404，确定检测到的是租用发生事件（lease issue）还是租用到期事件（leaseexpire）。

[0034] 如果被动分析工具 110 检测到租用到期事件，那么系统缓存就被访问，如步骤 406 所示。在判断步骤 408，确定与租用到期事件相关联的目标地址是否在系统缓存中被找到。如果在系统缓存中找到了目标地址，那么在步骤 410，该条目从系统缓存中被删除。然后被动分析工具 110 继续监视该 DHCP 服务器。如果在系统缓存中没有找到目标地址，那么该租用到期事件就被忽略，如步骤 412 所示。被动分析工具 110 继续监视 DHCP 服务器。

[0035] 回到判断步骤 404，如果检测到了租用发生事件，那么系统缓存就被访问，如步骤 414 所示。在判断步骤 416，确定与该租用发生事件相关联的目标地址是否在系统缓存中被找到。如果找到了目标地址，那么在步骤 418，该条目被删除。如果在系统缓存中没有找到该目标地址，那么继续执行该方法到步骤 420，如下所述。

[0036] 在步骤 420，目标主机的操作系统指纹在步骤 420 被获得。操作系统指纹在一特定期间被存储在系统缓存中，如步骤 422 所示。然后被动分析工具 110 继续监视 DHCP 服务器。

[0037] 图 4 所示的方法针对的是动态地向有防护网络 104 增加主机的过程，以使得关于网络的先验知识变得不再必要。这节省了大量时间和金钱，并且比需要网络先验知识的现有系统更精确。被动分析工具 110 可以将条目存储用户定义长度的时间，于是减少了需要获得操作系统指纹的次数，从而提高了网络入侵检测系统的效率。另一个技术上的优点是节省了资源，而且对有防护网络的影响很低，因为仅在需要时才建立目标系统的轮廓，从而有效率地进行“刚好及时”的易受攻击性分析。

[0038] 虽然本发明是结合若干示例性实施例进行描述的，但是，本领域的技术人员可以想到各种改变和修改。本发明希望包括这些落在本发明的权利要求范围之内的改变和修改。

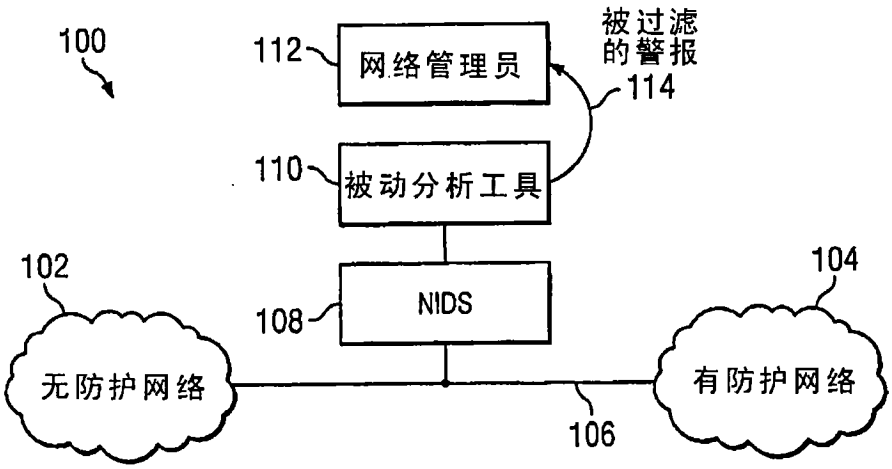

100
112
网络管理员
被过滤的警报
114
110
被动分析工具
102
104
108
NIDS
无防护网络
有防护网络
106

图 1

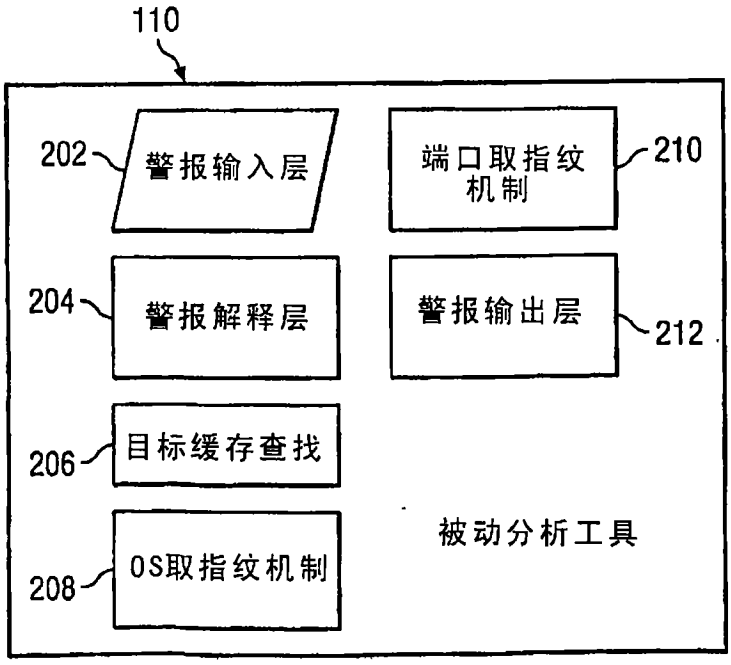

110
202
警报输入层
端口取指纹机制
210
204
警报解释层
警报输出层
212
206
目标缓存查找
208
OS取指纹机制
被动分析工具

图 2

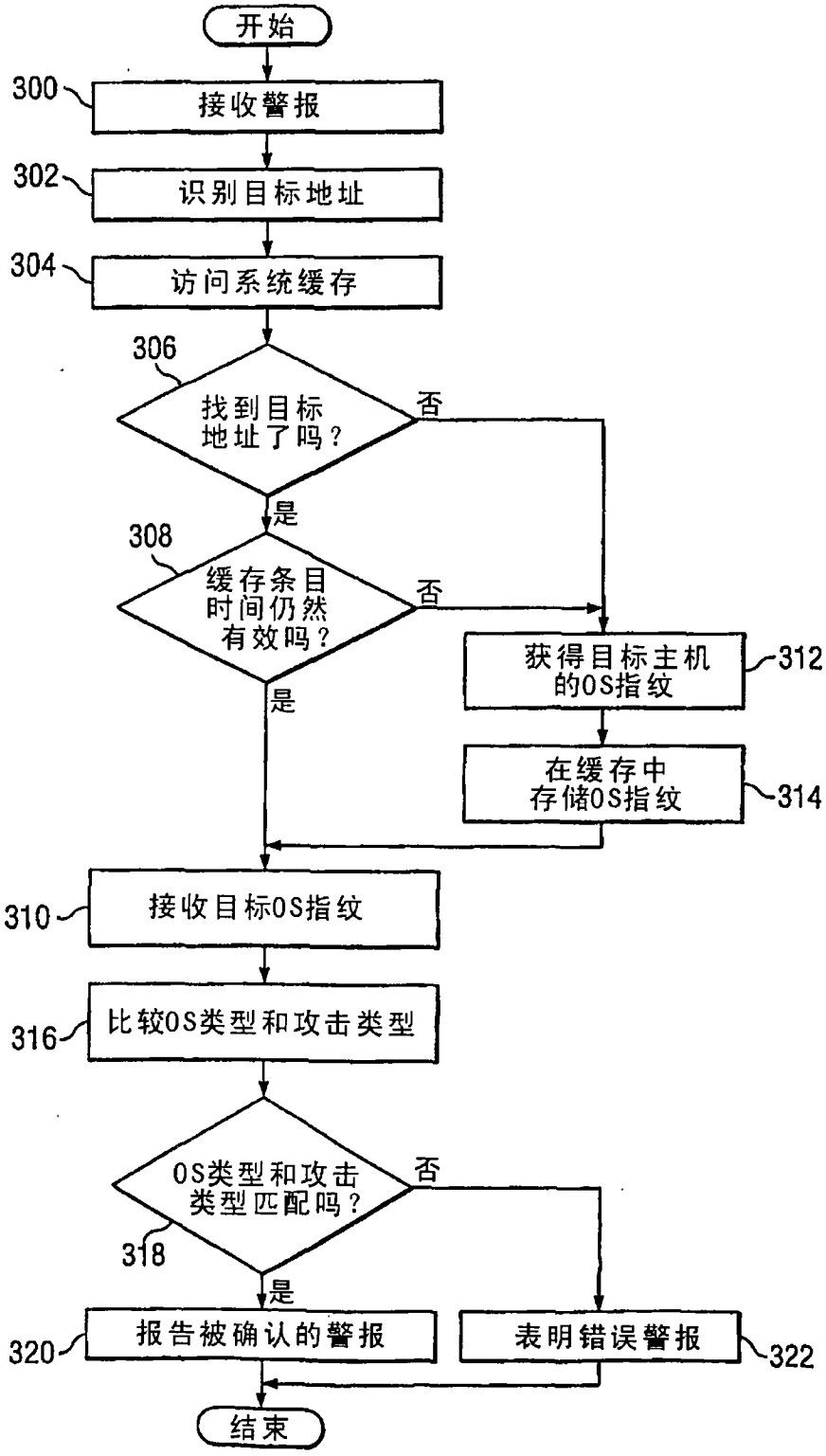

开始
300
接收警报
302
识别目标地址
304
访问系统缓存
306
找到目标地址了吗？
否
是
308
缓存条目时间仍然有效吗？
否
是
获得目标主机的OS指纹
312
在缓存中存储OS指纹
314
310
接收目标OS指纹
316
比较OS类型和攻击类型
OS类型和攻击类型匹配吗？
318
否
是
320
报告被确认的警报
表明错误警报
322
结束

图 3

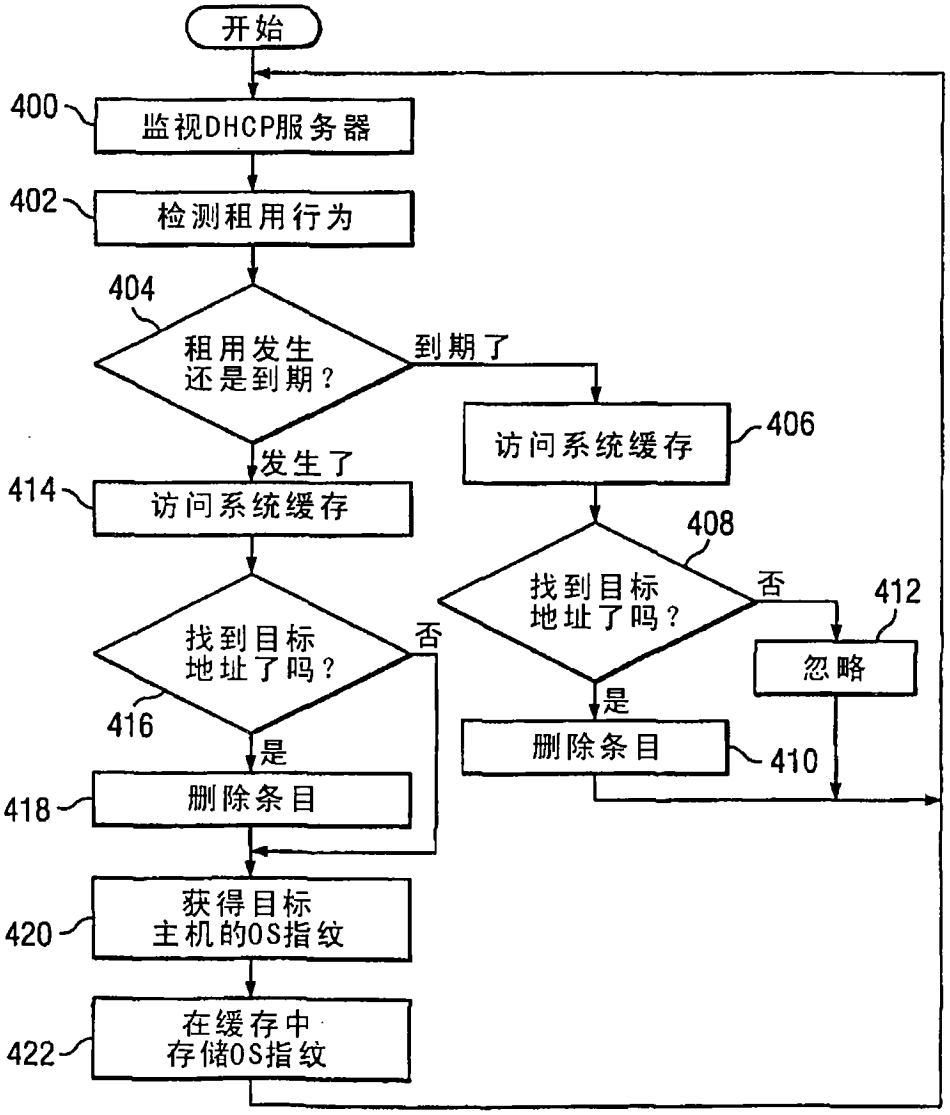

开始
400
监视DHCP服务器
402
检测租用行为
404
租用发生
还是到期？
到期了
发生了
406
访问系统缓存
414
访问系统缓存
408
找到目标
地址了吗？
否
412
忽略
是
删除条目
410
找到目标
地址了吗？
否
416
是
418
删除条目
420
获得目标
主机的OS指纹
422
在缓存中
存储OS指纹

图 4