(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 114254309 A
(43)申请公布日 2022.03.29

(21)申请号 202111586943.3

(22)申请日 2021.12.23

(71)申请人 江苏省未来网络创新研究院
地址 210000 江苏省南京市江宁开发区将军大道37号

(72)发明人 张广兴 姜海洋 廖志元 涂楚 谭航

(74)专利代理机构 北京卓岚智财知识产权代理事务所(特殊普通合伙) 11624
代理人 蒋真

(51)Int.Cl.
G06F 21/55(2013.01)

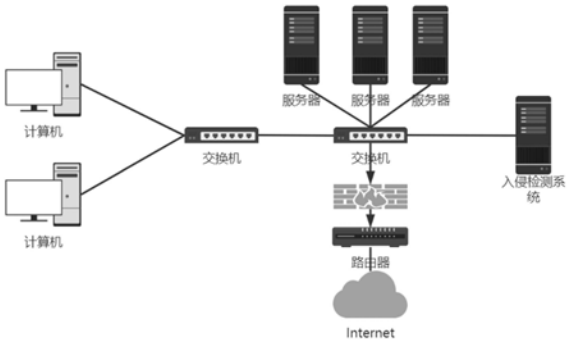
权利要求书1页 说明书4页 附图3页

(54)发明名称

一种记录与拾取过程分离的入侵检测系统的恶意载荷标注方法

(57)摘要

本发明提供了一种记录与拾取过程分离的入侵检测系统的恶意载荷标注方法，其特征在于，包括如下步骤：网络报文接入入侵检测系统，并完成解码和重组工作；报文重组模块在接受完单方向报文后，触发检测工作；攻击检测模块获取重组后包含恶意载荷的完整载荷内容，并从规则集中挑选预匹配规则序列；记录特征在重组载荷中的偏移、长度和类型；输出恶意载荷的偏移和长度。本发明首次提出了一种在入侵检测系统中对恶意载荷进行标注的方法；本发明将恶意载荷的记录和拾取过程进行分离，有效的降低攻击检测过程中对载荷的拷贝次数，降低入侵检测系统负载。



CN 114254309 A

1.一种记录与拾取过程分离的入侵检测系统的恶意载荷标注方法,其特征在于,包括如下步骤:

S1:网络报文接入入侵检测系统,并完成解码和重组工作;

S2:报文重组模块在接受完单方向报文后,触发检测工作;

S3:攻击检测模块获取重组后包含恶意载荷的完整载荷内容,并从规则集中挑选预匹配规则序列:signature0～signaturei,其中signaturek包含“ABC”、“DEF”两个恶意载荷特征;

S4:检测记录器在signaturek与重组载荷匹配成功“ABC”、“DEF”载荷特征时,记录特征在重组载荷中的偏移、长度和类型;

S5:载荷拾取器在检测完成后,根据检测的结果获取重组载荷与检测记录器数据结构,从重组载荷中获取恶意载荷内容“ABC”、“DEF”,并输出恶意载荷的偏移和长度。

2.根据权利要求1所述的记录与拾取过程分离的入侵检测系统的恶意载荷标注方法,其特征在于:所述步骤S4中,检测记录器具体过程为:

S4.1:攻击检测模块遍历signatur0～signaturei,取出signaturex,其中x∈[0,i];

S4.2:攻击检测模块将signaturex中的攻击特征与重组载荷进行对比;失败则返回上一步;

S4.3:比对成功,检测记录器记录第一个恶意载荷特征在重组载荷中的偏移位置,长度;循环比对规则中的下一个恶意载荷特征;比对失败则返回第一步;

S4.4:完成规则比对后记录器中已包含所有恶意载荷特征的偏移、长度、类型数据;进入拾取器模块;

S4.5:拾取器模块获取重组载荷、获取检测记录器数据结构,遍历检测记录器中恶意载荷的位置,将恶意载荷内容、偏移和长度信息拾取到日志文件中。

3.根据权利要求1所述的记录与拾取过程分离的入侵检测系统的恶意载荷标注方法,其特征在于:实现所述恶意载荷标注的系统包括:检测记录器模块和载荷拾取器模块,所述检测记录器模块用于在攻击检测模块检测过程中,记录检测过程中能够匹配规则中模式的恶意载荷偏移和长度;当检测结束后,如果报文匹配规则,则将检测记录器的结果送至载荷拾取器模块中,如报文未匹配规则,则释放检测记录器中已存放的恶意载荷信息;所述载荷拾取器根据检测记录的数据对恶意载荷进行拾取。

一种记录与拾取过程分离的入侵检测系统的恶意载荷标注方法

技术领域

[0001] 本发明涉及网络安全领域,具体涉及一种记录与拾取过程分离的入侵检测系统的恶意载荷标注方法。

背景技术

[0002] 恶意载荷,是网络攻击中对受害者造成伤害的攻击组成部分。对网络攻击中恶意载荷的分析已经成为入侵行为分析中不可或缺的部分。在基于签名的网络入侵检测系统中,签名中记录了大量预定义好的恶意载荷,攻击载荷由固定字符串或正则表达式组成用于描述符合特定约束条件的字符串。

[0003] 入侵检测系统在输入流量中通过与规则集中规则进行逐条比对来检测攻击行为。当检测到攻击行为后会输出告警日志。告警中包含入侵行为发生的时间、五元组信息、告警动作、告警ID等信息。网络安全管理员能够获取攻击行为的告警信息却无法将原始流量中包含的恶意载荷进行定位和提取。基于此,我们提出了一种入侵检测系统的恶意载荷标注方案,采用记录与拾取分离的方式,完成恶意载荷的标注功能。

发明内容

[0004] 本发明的目的是提供一种记录与拾取过程分离的入侵检测系统的恶意载荷标注方法,能够输出告警中恶意载荷在重组后载荷中的位置偏移,长度和具体内容。采用记录与拾取过程分离的设计可以有效的降低攻击检测过程中对载荷的拷贝次数,降低入侵检测系统负载。

[0005] 为实现上述目的,本发明采用了如下技术方案:

[0006] 一种记录与拾取过程分离的入侵检测系统的恶意载荷标注方法,其特征在于,包括如下步骤:

[0007] S1:网络报文接入入侵检测系统,并完成解码和重组工作;

[0008] S2:报文重组模块在接受完单方向报文后,触发检测工作;

[0009] S3:攻击检测模块获取重组后包含恶意载荷的完整载荷内容,并从规则集中挑选预匹配规则序列:signature0～signaturei,其中signaturek包含“ABC”、“DEF”两个恶意载荷特征;

[0010] S4:检测记录器在signaturek与重组载荷匹配成功“ABC”、“DEF”载荷特征时,记录特征在重组载荷中的偏移、长度和类型;

[0011] S5:载荷拾取器在检测完成后,根据检测的结果获取重组载荷与检测记录器数据结构,从重组载荷中获取恶意载荷内容“ABC”、“DEF”,并输出恶意载荷的偏移和长度。

[0012] 所述步骤S4中,检测记录器具体过程为:

[0013] S4.1:攻击检测模块遍历signatur0～signaturei,取出signaturex,其中x∈[0,i];

[0014] S4.2:攻击检测模块将signaturex中的攻击特征与重组载荷进行对比;失败则返回上一步;

[0015] S4.3:比对成功,检测记录器记录第一个恶意载荷特征在重组载荷中的偏移位置,长度;循环比对规则中的下一个恶意载荷特征;比对失败则返回第一步;

[0016] S4.4:完成规则比对后记录器中已包含所有恶意载荷特征的偏移、长度、类型数据;进入拾取器模块;

[0017] S4.5:拾取器模块获取重组载荷、获取检测记录器数据结构,遍历检测记录器中恶意载荷的位置,将恶意载荷内容、偏移和长度信息拾取到日志文件中。

[0018] 实现所述恶意载荷标注的系统包括:检测记录器模块和载荷拾取器模块,所述检测记录器模块用于在攻击检测模块检测过程中,记录检测过程中能够匹配规则中模式的恶意载荷偏移和长度;当检测结束后,如果报文匹配规则,则将检测记录器的结果送至载荷拾取器模块中,如报文未匹配规则,则释放检测记录器中已存放的恶意载荷信息;所述载荷拾取器根据检测记录的数据对恶意载荷进行拾取。

[0019] 所述检测记录器技术实现:

[0020] 采用对入侵检测模块扩展的方式,嵌入检测记录器模块。检测记录器模块采用链表数据结构形式完成对检测结果的记录。

[0021] 所述载荷拾取器技术实现:

[0022] 采用独立的拾取器模块实现方式,接入检测记录器模块之后。载荷拾取器模块采用在检测记录器完成记录后,统一进行恶意载荷拾取。

[0023] 与现有技术相比,本发明的有益效果在于:

[0024] 本发明首次提出了一种在入侵检测系统中对恶意载荷进行标注的方法。本发明将恶意载荷的记录和拾取过程进行分离,有效的降低攻击检测过程中对载荷的拷贝次数,降低入侵检测系统负载。

附图说明

[0025] 图1为现有技术中入侵系统检测流程图;

[0026] 图2为本发明恶意载荷标注的系统模块关系图;

[0027] 图3为本发明恶意载荷标注步骤示意图;

[0028] 图4为本发明入侵检测系统的典型部署示意图;

[0029] 图5为入侵检测系统检测记录器流程图;

[0030] 图6为入侵检测系统载荷拾取器流程图。

具体实施方式

[0031] 下面将结合本发明的附图,对本发明的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明的一部分实施例,而不是全部的实施例,基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明的保护范围。

[0032] 实施例

[0033] 一种记录与拾取过程分离的入侵检测系统的恶意载荷标注方法,其特征在于,包

括如下步骤：

[0034] S1:网络报文接入入侵检测系统,并完成解码和重组工作；

[0035] S2:报文重组模块在接受完单方向报文后,触发检测工作；

[0036] S3:攻击检测模块获取重组后包含恶意载荷的完整载荷内容,并从规则集中挑选预匹配规则序列:signature0～signaturei,其中signaturek包含“ABC”、“DEF”两个恶意载荷特征；

[0037] S4:检测记录器在signaturek与重组载荷匹配成功“ABC”、“DEF”载荷特征时,记录特征在重组载荷中的偏移、长度和类型；

[0038] S5:载荷拾取器在检测完成后,根据检测的结果获取重组载荷与检测记录器数据结构,从重组载荷中获取恶意载荷内容“ABC”、“DEF”,并输出恶意载荷的偏移和长度。

[0039] 如图5所示,所述步骤S4中,检测记录器具体过程为：

[0040] S4.1:攻击检测模块遍历signatur0～signaturei,取出signaturex,其中x∈[0,i]；

[0041] S4.2:攻击检测模块将signaturex中的攻击特征与重组载荷进行对比;失败则返回上一步；

[0042] S4.3:比对成功,检测记录器记录第一个恶意载荷特征在重组载荷中的偏移位置,长度;循环比对规则中的下一个恶意载荷特征;比对失败则返回第一步；

[0043] S4.4:完成规则比对后记录器中已包含所有恶意载荷特征的偏移、长度、类型数据;进入拾取器模块；

[0044] S4.5:拾取器模块获取重组载荷、获取检测记录器数据结构,遍历检测记录器中恶意载荷的位置,将恶意载荷内容、偏移和长度信息拾取到日志文件中。

[0045] 实现所述恶意载荷标注的系统包括:检测记录器模块和载荷拾取器模块,所述检测记录器模块用于在攻击检测模块检测过程中,记录检测过程中能够匹配规则中模式的恶意载荷偏移和长度;当检测结束后,如果报文匹配规则,则将检测记录器的结果送至载荷拾取器模块中,如报文未匹配规则,则释放检测记录器中已存放的恶意载荷信息;所述载荷拾取器根据检测记录的数据对恶意载荷进行拾取。

[0046] 所述检测记录器技术实现：

[0047] 采用对入侵检测模块扩展的方式,嵌入检测记录器模块。检测记录器模块采用链表数据结构形式完成对检测结果的记录。

[0048] 如图6所示,所述载荷拾取器技术实现：

[0049] 采用独立的拾取器模块实现方式,接入检测记录器模块之后。载荷拾取器模块采用在检测记录器完成记录后,统一进行恶意载荷拾取。

[0050] 部署方式:在入侵检测系统的典型部署示意图(图1)中,包含局域网计算机,服务器,交换机,防火墙,路由器,以及入侵检测系统服务器。入侵检测系统作为旁路设备,采集交换机镜像流量作为输入源,用于分析本网络环境中所有计算机、服务器的网络请求和交互流量。

[0051] 如图4所示,当入侵检测系统首次部署时,具体实施方法如下：

[0052] a.配置交换机镜像端口；

[0053] b.将交换机镜像端口连接至入侵检测系统流量采集网口；

[0054] c.配置入侵检测系统管理口IP地址；

[0055] d.登录入侵检测系统web客户端，检查入侵检测系统告警日志。

[0056] 以上显示和描述了本发明的基本原理、主要特征和本发明的优点。本行业的技术人员应该了解，本发明不受上述实施例的限制，上述实施例和说明书中描述的仅为发明的优选例，并不用来限制本发明，在不脱离本发明新型精神和范围的前提下，本发明还会有各种变化和改进，这些变化和改进都落入要求保护的本发明范围内。本发明要求保护范围由所附的权利要求书及其等效物界定。

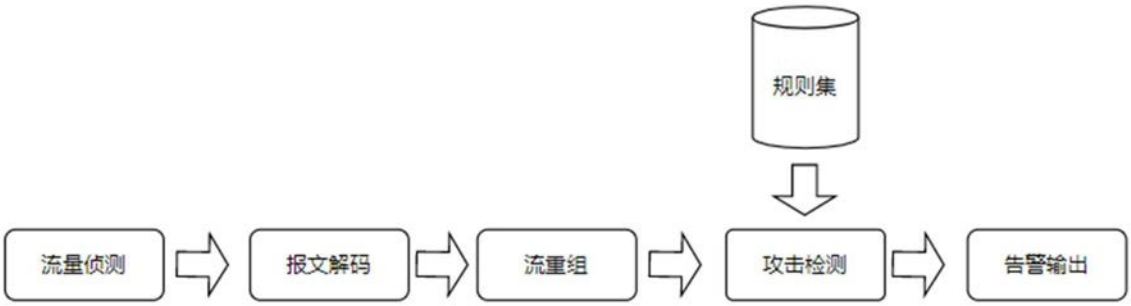

规则集
流量侦测
报文解码
流重组
攻击检测
告警输出

图1

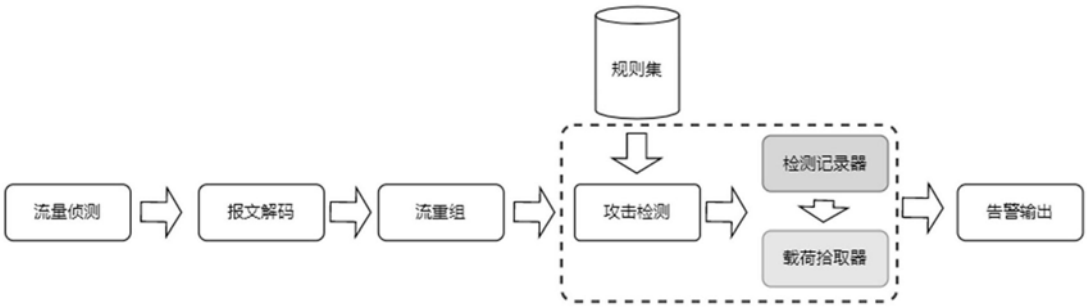

规则集
流量侦测
报文解码
流重组
攻击检测
检测记录器
载荷拾取器
告警输出

图2

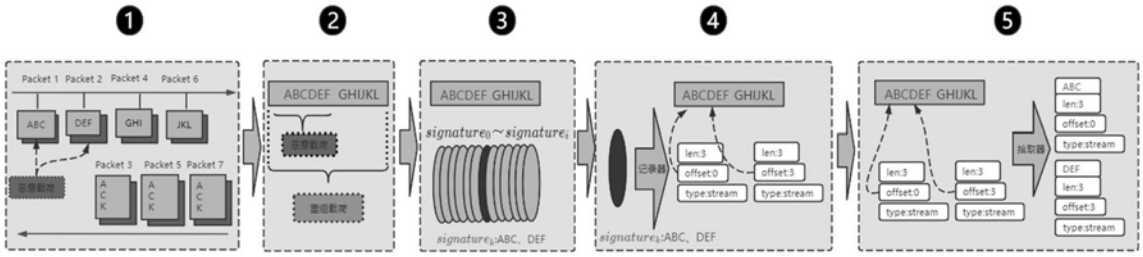

1
2
3
4
5
Packet 1 Packet 2 Packet 4 Packet 6
ABC
DEF
GHI
JKL
Packet 3 Packet 5 Packet 7
ACK
ABCDEF GHIJKL
signature0~signaturei
signature1:ABC、DEF
len:3
offset:0
type:stream
offset:3
ABC
DEF

图3

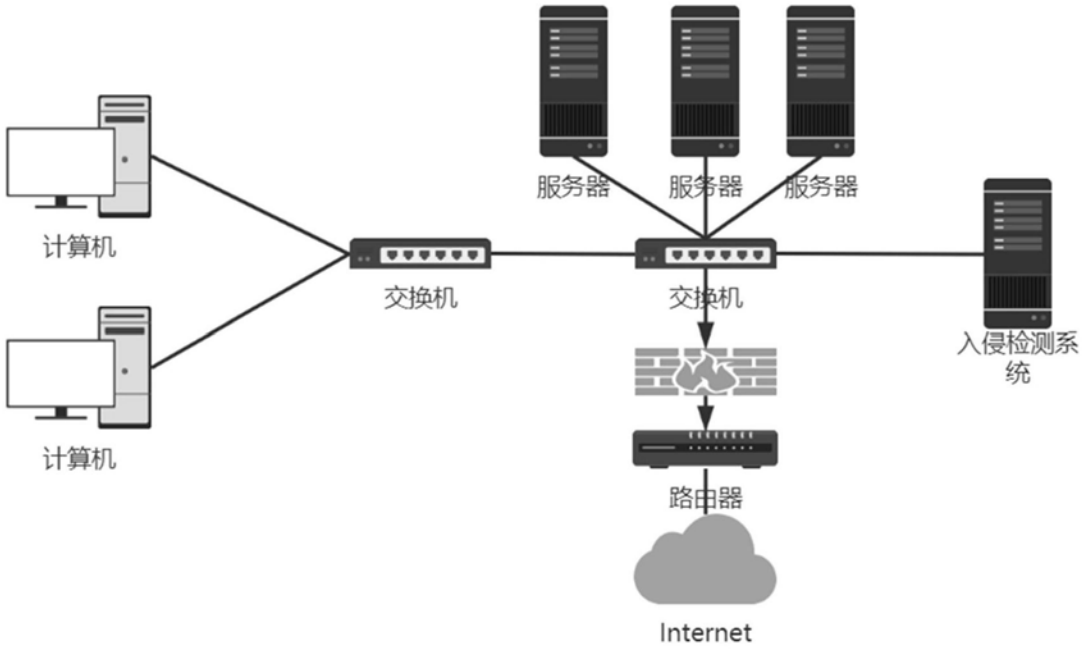

服务器
服务器
服务器
计算机
计算机
交换机
交换机
入侵检测系统
路由器
Internet

图4

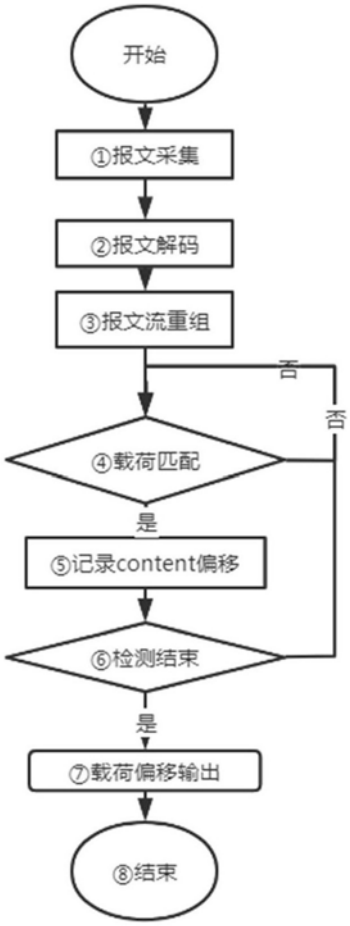

开始
①报文采集
②报文解码
③报文流重组
否
否
④载荷匹配
是
⑤记录content偏移
⑥检测结束
是
⑦载荷偏移输出
⑧结束

图5

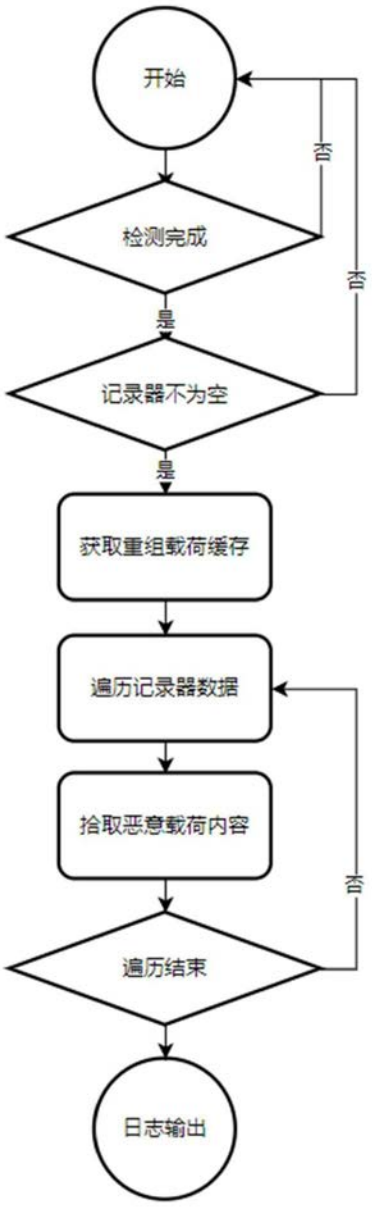


图6