



面向移动网络环境的智能协同蜜网设计与性能分析

陈利跃¹, 倪阳旦¹, 孔晓昀¹, 周升¹, 黄慧², 郑星³

- (1. 国网浙江省电力有限公司, 浙江 杭州 310007;
2. 国网浙江省电力有限公司丽水供电公司, 浙江 丽水 323000;
3. 国网浙江省电力有限公司衢州供电公司, 浙江 衢州 324000)

摘要: 在移动网络环境下, 因各移动蜜罐资源有限、攻击注入手段灵活多变, 需要动态部署蜜网以协同地检测攻击行为特征。然而现有蜜网易遭受特征识别攻击、网内恶意流量肆意传播、不能跨蜜罐迁移连接。为此, 基于软件定义网络 (software defined networking, SDN) 技术, 设计了一种智能协同蜜网 (intelligent and collaborative Honeynet, ic-Honeynet) 系统。它由逆向连接代理模块和蜜网控制器组成, 它的优势在于逐一克服了上述 3 个缺陷。最后, 搭建了一个 ic-Honeynet 实验环境, 并验证了该系统的有效性。实验结果表明: 该系统吞吐量近乎线速, 高达 8.23 Gbit/s; 响应时延额外增加很小, 仅在 0.5~1.2 ms 区间变化; 连接处理能力也很强, 可高达 1 473 个连接/s。

关键词: 蜜罐; 蜜网; 移动网络; 软件定义网络; 逆向连接代理

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018278

Design and performance analysis of a SDN-based intelligent and collaborative Honeynet for mobile networks environment

CHEN Liyue¹, NI Yangdan¹, KONG Xiaoyun¹, ZHOU Sheng¹, HUANG Hui², ZHENG Xing³

1. State Grid Zhejiang Electric Power Co., Ltd., Hangzhou 310007, China
2. State Grid Lishui Power Supply Company, Lishui 323000, China
3. State Grid Quzhou Power Supply Company, Quzhou 324000, China

Abstract: In the mobile network environment, the mobile honeypot resources are limited and the attack injection means are flexible, so it is necessary to dynamically deploy the honeynet to collaboratively detect the attack behavior characteristics. However, existing honey nets are susceptible to feature recognition attacks, malicious traffic within the network, and can't be migrated across honeypots. Based on software defined networking (SDN) technology, an intelligent collaborative honeynet system (ic-Honeynet) was designed. It consisted of a reverse connection proxy module and a honeynet controller. Finally, an ic-Honeynet experimental environment was built and the effectiveness of the system was verified. The experimental results show that the throughput of the system is nearly linear, up to 8.23 Gbit/s; the additional increase in response delay is small, only in the range of 0.5 to 1.2 ms; the connection processing capability is also very strong, up to 1 473 connections/s.

Key words: Honeypot, Honeynet, mobile network, software defined networking, reverse connection proxy

1 引言

蜜网作为一个分布式部署的多蜜罐系统,在引诱攻击者、获取攻击行为等方面,具有单蜜罐系统不可比拟的优势^[1],然而现有蜜网存在许多缺陷。不管是第一代蜜网 Gen-I,还是最新的第三代蜜网 Gen-III,它们在数据控制和数据捕获上存在较多的问题^[2]。首先它们对真实系统的服务或功能模仿逼真度不高而易受特征标识攻击;其次它们出/入流量控制机制不能阻止恶意流量在蜜网内部传播^[3];另外,它们也不能支持跨低交互型蜜罐(low interaction Honeypot, LIH)和高交互型蜜罐(high interaction Honeypot, HIIH)无缝间连接动态切换^[4]。现有蜜网却无法有效利用 LIH 和 HIIH 各自的优势^[5],更无法适应移动网络环境需求:首先在传统蜜网中蜜罐常部署在有限几个固定网络节点,无法对无网不入的移动攻击流量实施无遗漏的捕获;其次传统蜜网仅能对连接持续时间长、连接蜜罐对象固定的攻击流量进行特征提取,而无法有效地监测和捕获移动游牧式或大量短时攻击流量^[6-8],造成现有蜜网在移动环境下的攻击行为特征捕获效率低下。

由于 SDN 可以实现集中式的网络管理,SDN 控制器可以对联网设备的路由策略进行集中配置^[9]。为了解决当前蜜网面临的问题,基于 SDN 技术,重新设计了一种新的智能协同蜜网体系结构(ic-Honeynet)。该结构不仅解决了特征识别攻击、网内恶意流量肆意传播、不能跨蜜罐迁移连接的 3 个问题,而且还实现了一种支持透明、多播、中继 3 种连接操作模式的连接管理引擎。最后,ic-Honeynet 原型系统的实验结果表明:该系统的 TCP 吞吐量能获得 8.23 Gbit/s 近似线速的吞吐量,而不同连接操作模式引入的平均时延为 0.5~1.2 ms,每秒能处理的连接数为 640~1 473。

2 现有蜜网缺陷

针对移动网络环境,当前蜜网还存在不少缺陷:首先易遭受特征标识攻击,即通常它们是模仿实际系统,以此作为攻击诱饵,但常被攻击者识破;其次无法阻止网内恶意流量肆意传播,而造成蜜网内一个蜜罐被攻陷,其他的蜜罐也相继沦陷;最后,缺乏跨蜜罐的连接切换支持机制,无法发挥不同类型蜜罐各自的优势。

首先,现有蜜罐的最大缺陷在于:易受特征标识攻击。因它们对真实系统的服务或功能模仿逼真度不高,使得攻击者很快识破蜜罐系统,而放弃对蜜罐的攻击。例如:现有的 SSH 蜜罐 Kippo^[11],攻击者用 Linux 命令“uname-a”就能轻松地获取该系统的特征标识,而很快辨识出该系统是一个蜜罐系统。因为 Kippo 通过输出一个硬编码的时间戳“Wed Nov 4 20:45:37 UTC 2009”来简单模仿“uname”命令的输出信息。

其次,现有蜜网不能有效监控内部流量,因为它们常将用户网关 Honeywall 部署在网络中的固定位置,而无法对全网域内的流量进行有效监控。一旦某个蜜罐被攻陷,其产生的恶意流量就会在网内肆意传播,而感染网内的其他蜜罐。

最后,当前蜜网仅让攻击者与相关蜜罐独自建立单一连接,而没有协同地利用 LIH 和 HIIH 各自的优势,使得蜜网的攻击者捕获性能完全受限于各蜜罐自身能力大小。实际上,可以协同地利用两类蜜罐。例如:在扫描攻击时或一个攻击的登录阶段,先指派使用 LIH 蜜罐;而在登录成功后,再激活 HIIH,为攻击者提供更活跃的交互操作。虽然 Honeybrid 支持 LIH 和 HIIH 间的连接切换,实现了两类蜜罐的高效使用^[11]。然而,该系统无法灵活地配置何时以及怎样将攻击者与蜜罐之间已建立的连接从一个蜜罐切换到另一个蜜罐。



3 ic-Honeynet: 智能协同蜜网系统设计

为了解决现有蜜网的上述 3 个缺陷, 基于 SDN 技术, 提出了一种智能协同的蜜网系统 ic-Honeynet。下面将首先阐述该系统的设计目标和原则, 然后描述该系统的总体设计与考虑, 再详细阐述该系统的结构组成及功能实现。

3.1 新型蜜网系统的设计要求

一个理想的蜜网系统, 应满足如下设计目标和原则。一是监控全网域覆盖: 蜜网系统要能监控所有的网络内部流量, 以防止被攻陷蜜罐在网络内部传播其恶意流量; 其次, 它能实现集中化的网络监控以及全网域的策略执行。二是蜜罐资源协同利用: 蜜网系统必须支持 LIH 和 HIH 之间的无缝切换, 而且该切换也必须灵活和可配置。三是蜜罐高隐蔽性部署: 蜜网系统必须具有一定的隐蔽性, 即它必须既能对外隐藏自己的存在, 也要尽可能最小化地暴露蜜网内的蜜罐系统。因此, 这要求蜜网在执行给定任务时, 不能引起时延的显著变化, 因为时延变化较大就可能导致蜜网被攻击者检测。四是一般化, 不管蜜网内蜜罐类型如何, 也不管运行什么服务, 蜜网系统都要可用。因此, 蜜网系统要能有效协调不同蜜罐系

统提供的冗余服务。

3.2 ic-Honeynet 系统总体设计与考虑

从结构上看, ic-Honeynet 蜜网系统由逆向连接代理模块和蜜网控制器(即一个 SDN 应用)组成, 其中蜜网控制器与 SDN 控制器一起协同地执行相应的安全规则和网络规则。多个蜜罐可以连接到不同的 SDN 交换机, 但是它们都受 ic-Honeynet 控制器的集中管理。攻击者发出的访问请求将经过逆向代理中一系列模块的处理之后, 再转发到一系列相关蜜罐系统中。

如图 1 所示, 逆向代理首先提取分组头中特定的标记信息, 然后 ic-Honeynet 控制器生成相应的 SDN 流规则, 并查验 SDN 交换机上的标记信息以执行相应的网络流量控制策略。代理模块具有 3 种操作模式, 根据控制器的决策, 按需地配置相应的操作模式。为了阻止特征标识攻击, 代理模块将检查响应消息的净荷, 重点检查其中是否含有任何可能暴露部署有蜜网/蜜罐的特征标识。一旦发现这样的标识, 代理将立即通知控制器采取相应动作, 例如改变代理模式或更新网络配置。代理模块也负责处理加密通信, 如 SSH (secure shell) 连接。

图 2 给出了 ic-Honeynet 如何改变蜜网的设计

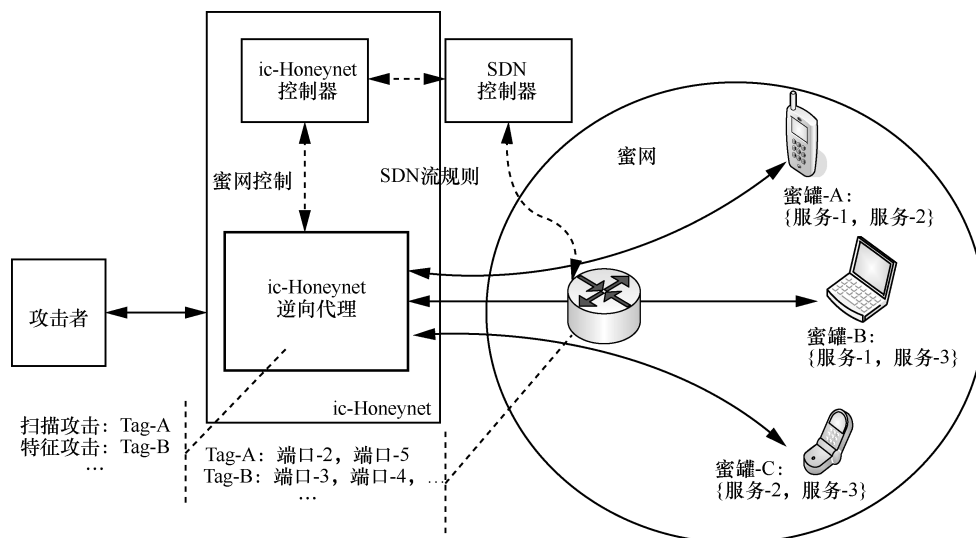


图 1 ic-Honeynet 蜜网系统总体结构示意图

理念。传统的蜜网体系结构是在用户防火墙 Honeywall 之后运行多个蜜罐系统。然而,传统的体系结构可能出现同一个模仿服务大量冗余,因为这些蜜罐间缺乏交互,如图 2 (a) 所示。这实际上就是它们数据控制低效的原因,因为攻击者在任何时候仅能访问一个蜜罐。由于蜜罐间缺乏有效的切换支持机制,每个蜜罐需要大量的手工配置以模仿所有可能的服务,这也是传统蜜网中存在大量冗余服务的主要原因。

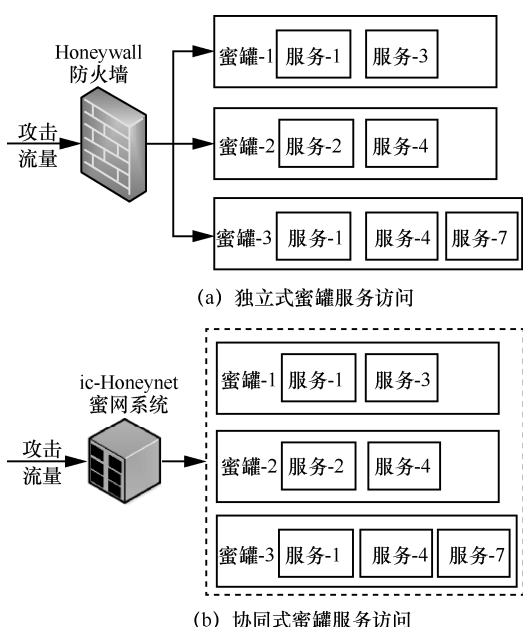


图2 蜜网体系结构设计理念的变革

如图 2 (b) 所示,在 ic-Honeynet 结构下,运行的多个蜜罐可以视为一个大型蜜罐系统,其上运行了多个脆弱性服务。因此,它不必增加额外负担去跨多个不同的蜜罐运行多个冗余服务,因为代理模块将攻击者的访问请求分发到相关蜜罐,然后从多个响应中选择最优的一个。换言之,攻击者不能通过一个蜜罐来确定另一个蜜罐,它仅能将蜜网当作一个蜜罐系统。为了有效地生成多播消息,代理模块将在内部实现网络地址转换 (network address translation, NAT) 和深度分组检测 (deep packet inspection, DPI) 功能,以支持同一服务跨蜜罐互连。

3.3 ic-Honeynet 系统结构组成及主要功能实现

智能协同的蜜网系统 ic-Honeynet 的结构如图 3 所示,它包含逆向代理模块和 SDN 应用 (即 ic-Honeynet 控制器)。它在设计中,将网络可控编程与分组处理分为两个不同的逻辑层。在逆向代理模块中,它的请求处理器 (request handler)、连接管理引擎 (connection management engine)、响应清洗器 (response scrubber) 3 个子模块处理出/入流量,而网络配置管理、SDN 规则执行、可疑流量监控等功能则由 ic-Honeynet 控制器完成。

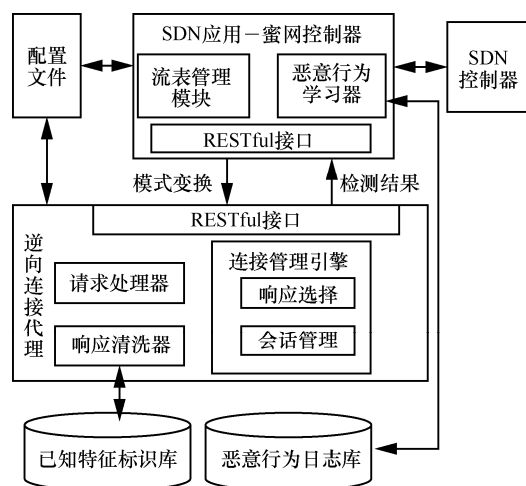


图3 ic-Honeynet 蜜网系统的功能性结构

请求处理器子模块:它负责监控和检查输入流量中的可疑分组,并通知连接管理引擎其检查结果。当它收到一个分组时,首先检查净荷是否含有任何已知特征标识攻击。若净荷含有扫描攻击,则请求处理子模块将为该分组添加上“scanning”标签,并将该分组向运行有入侵检测系统 (IDS) 服务的蜜罐转发。此外,该子模块将根据净荷检查结果,通知连接管理引擎执行 NAT 和 DPI 等操作以管理攻击者的访问会话连接。

连接管理引擎:是逆向代理模块的核心子模块,由它协调处理攻击者访问请求和攻击响应。它的主要目的是从来自多个蜜罐的攻击响应中优选一个响应,并以 3 种操作模式管理和维持攻击会话连接。同时该子模块也向输入流量分组头添



加标签信息,以便 SDN 交换机将这些分组转发到匹配的目的蜜罐系统。

响应清洗子模块:它负责检测蜜罐发出的攻击响应中是否含有特征标识。若响应中包含有特征标识,则它将通知 ic-Honeynet 蜜网控制器。该子模块主要操作如下:首先它将来自相应蜜罐的攻击响应依次地记录在队列 R_Queue 中,直到该队列长度等于相应蜜罐数。若它们两者相等或队列定时器超时前 R_Queue 长度还没有达到蜜罐数,则连接管理引擎将从队列 R_Queue 中优选一个攻击响应作为攻击者攻击访问请求的响应。

流表管理子模块:它是 ic-Honeynet 控制器的一个组成部分,它负责通知控制器为逆向代理处理的特定流量添加 SDN 规则,即流表项。例如:针对被请求处理子模块标记为“scanning”的分组流,控制器将为其生成相应的流表,并将该流表下发到 SDN 交换机,然后交换机将这些分组流以多播形式转发到多个部署有入侵检测系统(如 snort)的蜜罐系统,以便能有多个蜜罐系统同时对攻击者的攻击访问请求做出响应。

连接操作模式决策子模块:它确定逆向代理的攻击者与蜜罐间连接管理操作模式。它可以基于几个准则,向逆向代理发起请求以变换操作模式。

为了满足第一个设计目标,即普适性,ic-Honeynet 利用了 SDN 技术动态地变换其连接管理操作模式,并由 SDN 控制器执行相应的流表和网络安全规则管理。它能够通过 SDN 控制器监控网络中所有的数据流,因此被攻陷的蜜罐发起的任何连接企图都将被记录、监控、阻止。为了支持蜜罐间无缝切换,即满足第二个设计目标——灵活性,连接管理引擎从攻击响应记录队列 R_Queue 中优选一个最合适的响应,并跟踪所有活跃连接的状态变化。此外,ic-Honeynet 还能透明地将连接从一个蜜罐迁移到另一个蜜罐。为了

满足第三个目标,即隐匿性,ic-Honeynet 利用多进程技术,可最小化不同连接管理操作模式间的性能差异,例如:不同模式间的时延差 $<1\text{ ms}$,这很难让攻击者区分出来。为了满足最后一个设计目标,即一般化,ic-Honeynet 可与相关的蜜罐建立起多个套接字(socket),以支持 OSI 四层及更高层的多个应用连接。因为除了扫描攻击外,其他的脆弱服务大多使用七层的应用层协议,因此 ic-Honeynet 可以支持更多的协议。而对于利用三层及以下协议的扫描攻击,ic-Honeynet 仅需将攻击分组重定向到部署有 IDS 的蜜罐。

4 ic-Honeynet 的连接管理机制设计与连接管理操作模式切换

为了更好地监测移动网络环境下输入蜜网的攻击流量和蜜网内被攻陷蜜罐产生的恶意流量,设计了一种基于攻击进展状态的自适应连接管理机制。该机制运行在连接管理引擎,它的核心在于 3 种连接管理操作模式,即透明模式(T-mode)、多播模式(M-mode)、中继模式(R-mode)。这些模式的主要任务在于:如何高效地将攻击者的恶意流量分发给相关蜜罐,并从众多蜜罐发出的攻击响应中优选最佳的一个作为攻击者访问请求的响应。

4.1 连接管理操作模式

为了更好地阐述连接管理机制,图 4 给出了这 3 种操作模式间关系以及它们的切换逻辑,它们各自的主要功能和操作如下。

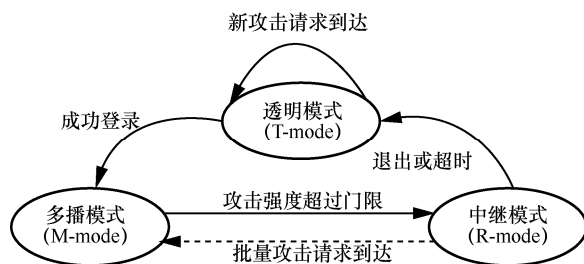


图 4 ic-Honeynet 蜜网系统的 3 种连接管理模式及切换逻辑

- 透明模式 (T-mode): 它主要用在攻击的初始阶段, 如登录企图。因为这些攻击企图常以自动方式发起, 低交互蜜罐就能有效对付这些攻击。考虑到可扩展性, ic-Honeynet 在这种模式下仅执行网络地址转换而不执行深度分组检测。
- 多播模式 (M-mode): 一旦攻击者登录成功, ic-Honeynet 为了对抗特征标识攻击, 需将操作模式从透明模式变换到多播模式。在 M-mode 下, 每一个输入分组被转发到所有的相关蜜罐系统。然而, 此时仅发送多播消息是不够的, 因为每个会话还有各自不同的会话变量, 例如: cookie 或共享会话密钥, 它们由两端蜜罐系统生成和管理。为此, ic-Honeynet 将构造多个套接字以维护蜜罐与 ic-Honeynet 间的多个连接, 并记录这些连接相关的会话数据。后面将详细阐述 ic-Honeynet 如何维护多个会话数据以及如何从所有收到的响应中选择一个最佳的响应转给攻击者。
- 中继模式 (R-mode): 一旦收到 ic-Honeynet 控制器发出的模式变换指令, ic-Honeynet 需将操作模式从 M-mode 变换到 R-mode, 或从 R-mode 变换到 M-mode。该模式本质上仅考虑维持一个由 HIH 建立的连接同攻击者进行交互, 而其他连接则被暂时性地挂起。实际上, 让具有很强攻击目的性的

攻击者仅与 LIH 间长期保持连接, 这是不可行的。在这种情形下, ic-Honeynet 就不必再承担 M-mode 带来的管理负担, 即发送多播消息给相关蜜罐。因此通过将其余的会话配置为 Standby 状态, R-mode 可以极大降低连接管理开销, 提升 ic-Honeynet 对攻击者攻击行为的监控性能和效率。当确有必要时 (例如: 攻击者发出了大量请求, 并超过了预设门限), 控制器可以发出变换指令, 让操作模式从 R-mode 切换回 M-mode, 并让 LIH 与攻击者交互。

4.2 响应优选与会话管理

对可能暴露蜜罐存在或蜜网结构核心信息的特征标识, ic-Honeynet 收集并维护了一个已知蜜罐特征标识数据库, 并将其反馈给 ic-Honeynet 控制器, 供模式决策模块使用。例如: 针对 SSH 蜜罐 Kippo, 参考文献[11]列出了所有已知的 Kippo 蜜罐特征标识。实际上, 为了有效防止向攻击者发送含有确定特征标识的攻击响应, ic-Honeynet 的逆向代理模块可以从多个响应中选择一个不含有这些标识的响应。

ic-Honeynet 以结构化方式管理多个会话。当它建立一个与攻击者的会话时, 它将与相关蜜罐一起内部生成相应的会话号。图 5 给出了在 M-mode 模式下, 多个活跃套接字如何维护“一对多 (1:N)”会话连接, 其中 Socket0 对应于攻击者发起到逆向代理模块的连接, 而其余的连接则对

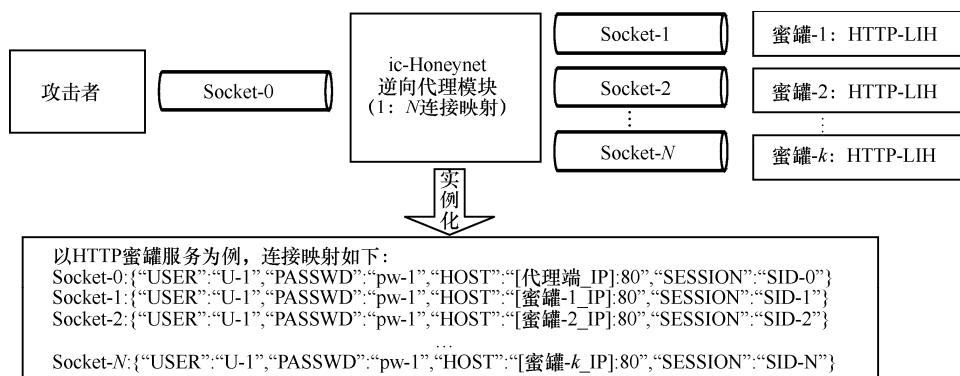


图 5 多播模式下“一对多 (1:N)”套接字映射示意图



应于逆向代理模块发起到 N 个提供有脆弱服务的蜜罐的会话连接。这里，每个连接都由逆向代理模块的连接管理引擎子模块集中管理。逆向代理模块也管理着攻击者的标识（如 HTTP 会话的 cookie 信息、SSH 会话连接的共享会话密钥等），以便 ic-Honeynet 能重写攻击者的 Socket，使蜜罐上配置的脆弱服务能收到攻击者发出的攻击分组。

4.3 ic-Honeynet 控制器的连接管理操作模式变换准则

针对攻击者的攻击访问请求，高交互性蜜罐服务（即是否应以 R-mode 模式操作）需要作出合理的响应决策。这里，设计了一套决策策略，其中决策依据主要包括当前连接持续时间 δ_l 、当前特征标识攻击次数 δ_c 以及每个攻击者的历史记录 <连接持续时间总和 R_l ，攻击次数总和 R_c >。这些历史记录常通过 IP 地址进行查找，因为具有相同标识（即“用户名—密码”组合）通常意味着也具有相同的 IP 地址。对于那些已访问蜜网的攻击者，把它们的访问记录保存在恶意行为日志库。ic-Honeynet 可从该库中查询历史记录，并依据这些记录作决策而更好地收集攻击者相关信息。若把针对会话 s 的操作模式决策定义为模式决策函数 $f_m()$ ，则该函数可表示为：

$$f_m(s) = \begin{cases} \text{R-mode}, & \frac{R_l}{R_l + \delta_l} \cdot R_c + \frac{\delta_l}{R_l + \delta_l} \cdot \delta_c \geq \theta \\ \text{M-mode}, & \text{其他} \end{cases} \quad (1)$$

其中，门限值 θ 主要用于平衡 LIH 和 HIH 不同类型蜜罐之间的负载。

5 流表管理机制

ic-Honeynet 充分利用了 SDN 高度可编程性，由其连接管理引擎对输入分组进行分类，并给每类分组添加上相应的标签。依据这些不同标签，SDN 控制器将采取不同的方式处理这些分组。

5.1 流表管理

可对输入分组进行分类和添加标签，并依据标签对各分组采取不同的路由策略。这里，首先由请求处理子模块确定输入流量里是否含有“扫描攻击”，然后连接管理引擎对其余分组再进一步分类。同时，蜜网中各蜜罐部署了各不相同的脆弱服务。假设输入分组的类别集合为 $T = \langle \text{scanning, fingerprinting, ...} \rangle$ ，脆弱服务集合为 $S = \langle \text{ssh, http, database, ftp, ...} \rangle$ ，则 SDN 控制器可以为输入流量生成多达 $|T| \cdot |S|$ 条 SDN 规则（即流表）。模式决策模块保存这些 SDN 规则，并利用这些规则对攻击者作相应的处理。

5.2 阻止恶意流量网内传播方案

为了阻止恶意流量在网内部肆意传播，传统蜜网采取的方案是：在各蜜罐添加基于主机的访问控制规则（如 iptables）。然而一旦某一个蜜罐被攻陷，攻击者则可以绕开这些访问控制规则。鉴于此，为了有别于传统的主机级阻止方案，ic-Honeynet 则提出了基于全网域监控的阻止方案：访问控制规则在控制器的统一管理下，按需地分发到蜜网中相应的 SDN 交换机，再由 SDN 交换机将不同的数据流转发到相应的蜜罐系统。因此，即使是蜜网内各蜜罐间的数据流，也被 ic-Honeynet 纳入监控，从而有效检测恶意流量网内传播。这里因输入分组要经过 IDS 处理，而且输入流量和输出流量分别按不同的 SDN 规则处理，使得它们彼此间可能物理隔离，其传输路径不一定相同。显然，该方案对网络管理者非常重要：不仅能管理整个蜜网，而且还能实时发现网内的安全违例情形。

6 实验环境下 ic-Honeynet 主要性能测试与分析

6.1 ic-Honeynet 实验环境设置与性能评估指标确定

如图 6 所示，利用两台物理主机搭建了一个 ic-Honeynet 蜜网实验环境，其中以 POX 为基础实

现 SDN 控制器, 以 OpenSwitch 软件实现 SDN 交换机, 以 KVM 虚拟机方式安装运行多个虚拟蜜罐系统。在该蜜网实验环境中, 分别配置了 LIH 和 HIH 两类蜜罐, 并各自部署 HTTP 和 SSH 两类典型服务。针对 HTTP 服务, 分别选择了广泛部署应用的 LIH 蜜罐系统 Glastopf 和 HIH 蜜罐系统 HIHAT; 而针对 SSH 服务, 也选择了常用的 LIH 蜜罐系统 Kippo 和 HIH 蜜罐系统 OpenSSH。这里, 物理主机是两台 CPU 为 Intel Xeon (E5-2658v3 @2.20 GHz、24 核)、内存为 128 GB 高性能台式计算机, 其操作系统为 Ubuntu 16.04 LTS, 其 Linux 内核为 4.4.0 版本; SDN 软交换机为 OpenSwitch v2.5.0; 每个虚拟蜜罐主机配置 4 个虚拟 CPU、4 GB 虚拟内存, 每个蜜罐主机的线速最大为 10 Gbit/s。

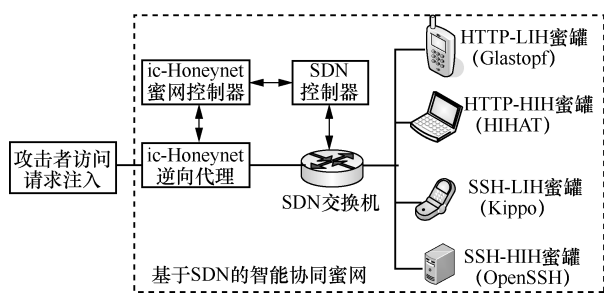


图6 ic-Honeynet 蜜网实验环境设置

监控和分析输入和输出分组净荷需要相当多的资源。尤其, 当分组到达逆向代理模块时, ic-Honeynet 需要与已知特征标识攻击的特征标识逐一进行比较, 显然它在攻击访问请求的处理能力可能会存在瓶颈。因此, 需要评估 ic-Honeynet 的性能及处理开销以及它们对攻击者行为的影响。这里, 从如下 3 个方面进行评估: 一是吞吐量 (单位: Gbit/s), 即单位时间内的数据处理能力; 二是时延大小 (单位: ms), 尤其是以不同模式处理攻击访问请求时的时延差异; 三是每秒的连接处理能力 (单位: 连接数/s)。

6.2 ic-Honeynet 系统主要性能

首先, 从吞吐量角度来评估其性能。图 7 给

出了基于 iperf 测试工具获得的 ic-Honeynet 在 HTTP 和 SSH 等服务情形下的吞吐量结果。在 T-mode 模式下, 它的 TCP 吞吐量可达 8.23 Gbit/s, 而在 M-mode 和 R-mode 模式下分别为 4.5 Gbit/s 和 7.79 Gbit/s。与其他两种模式相比, M-mode 模式的吞吐量要低许多。这是因为该模式下, 代理模块要为生成多个攻击访问请求分组副本, 并发送多播消息, 这需要消耗大量的资源。此外, 它的 SSH 蜜罐服务情形下吞吐量比 HTTP 约低 57%, 因为它要处理数据的加/解密。

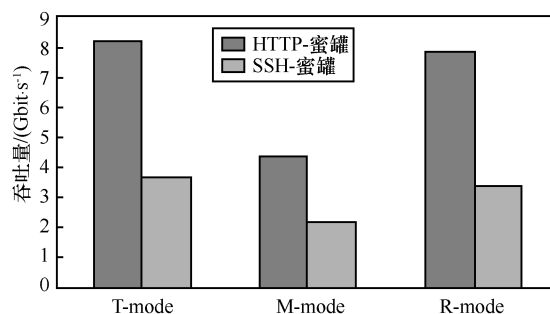


图7 ic-Honeynet 蜜网吞吐量性能

其次, 从时延角度评估 ic-Honeynet 的性能, 因为时延能反映攻击者和蜜罐间端到端响应的快速性和及时性, 而前面的吞吐量则主要反映了 ic-Honeynet 的批量数据传输性能。这里, 时延是以客户端与服务器之间的往返时间 RTT 为基础来测量的。为了便于对比, 测量了 4 种情形下的时延变化: 一是在蜜网中关闭 ic-Honeynet, 让攻击者直接访问任意蜜罐; 二是蜜网分别以 T/M/R 3 种模式运行, 访问部署有 HTTP 的蜜罐系统。时延测量结果如图 8 所示, 攻击者客户端与蜜罐间的 RTT 时延平均为 0.5 ms, 而当开启 ic-Honeynet 时, 其平均 RTT 时延在 1~1.7 ms 区间变化, 其中 T-mode 为 1.24 ms、M-mode 为 1.50 ms、R-mode 为 1.32 ms。由此可知: 开启 ic-Honeynet 后, 它的时延仅小幅度增加, 其幅度在 0.5~1.2 ms 内变化。时延小幅变化, 可以使攻击者察觉不到 ic-Honeynet 蜜网的存在, 因此满足蜜网的隐匿性设计要求。

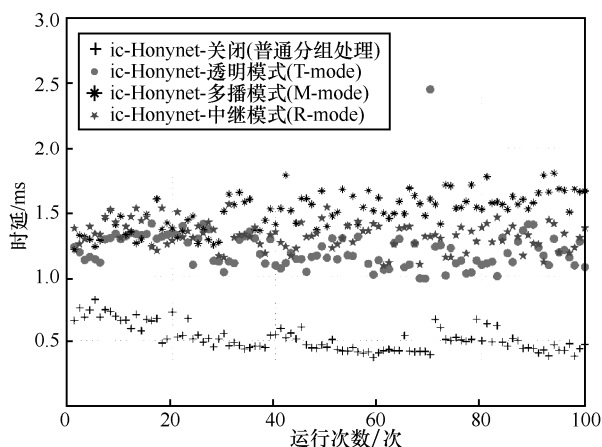


图8 ic-Honeynet 蜜网时延性能

再次,从连接处理能力角度评估其性能。它反映了 ic-Honeynet 对攻击访问请求的处理能力,因为对每个攻击访问请求,ic-Honeynet 都需要在攻击者与蜜罐间为其建立连接,并对该连接进行管理和维护。在 60 s 时间间隔内,输入和输出连接(具有纳秒时间精度)被持续地记录。当 ic-Honeynet 没有开启时,系统的连接处理能力全取决于蜜罐自身的能力。如图 9 所示,此时 HTTP 蜜罐和 SSH 蜜罐的连接处理能力分别为 2 500 个连接/s、2 410 个连接/s。当 ic-Honeynet 开启时,针对部署有 HTTP 服务的蜜罐,在 T/M/R 3 种模式下,蜜网系统的连接处理能力分别为:1 473 个连接/s、1 058 个连接/s、1 443 个连接/s;而针对部署有 SSH 服务的蜜罐,在 T/M/R 3 种模式下的处理能力分别为:1 000 个连接/s、640 个连接/s、917 个连接/s。性能指标的变化与吞吐量的变化一致,M-mode 模式下的连接处理能力比其他两个模式均要低,这主要原因在于:M-mode 模式要对输入流量进行多播处理,消耗了逆向代理模块的处理资源。与普通情形(即不启用 ic-Honeynet)相比,蜜网系统在任意模式下的连接处理能力都降低了,其幅度为 41%~55%。鉴于 3 种模式下的连接处理能力相差不大,因此攻击者很难辨识出 ic-Honeynet 工作于哪一种连接管理模式,这满足了蜜网设计的隐匿性要求。

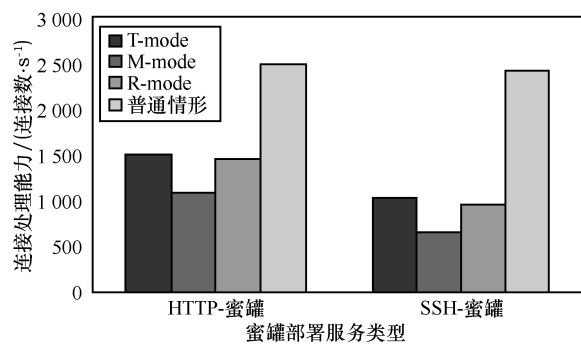


图9 ic-Honeynet 蜜网的连接处理能力

7 结束语

本文针对移动网络环境下攻击检测面临的技术挑战,基于 SDN 技术在网络全局视图、全网域集中控制等方面具有的优势,设计了一种新的蜜网系统,即 ic-Honeynet。与传统蜜网系统相比,设计的蜜网系统具有如下优势:该系统能允许攻击者访问多个脆弱性服务,从而诱导它与多个蜜罐产生更多、更深入的交互,并让网络管理者可以收集攻击者更多的恶意行为数据。通过动态选择最优攻击响应,可以减轻特征标识攻击带来的影响。SDN 控制器能监控全网域内的蜜罐,能有效发现蜜网内出现的任何异常行为,如通过监控蜜罐间的连接尝试次数等,这样就能事先阻止恶意流量在网络内的肆意传播。

参考文献:

- [1] 贾召鹏,方滨兴,刘潮歌,等.网络欺骗技术综述[J].通信学报,2017,38(12):128-143.
JIA Z P, FANG BX, LIU C G, et al. Survey on cyber deception[J]. Journal on Communications, 2017, 38(12): 128-143.
- [2] 诸葛建伟,唐勇,韩心慧,等.蜜罐技术研究与应用进展[J].软件学报,2013,24(4):825-842.
ZHUGE J W, TANG Y, HAN X H, et al. Honeypot technology research and application[J]. Journal of Software, 2013, 24(4): 825-842.
- [3] THOMPSON M F. Effects of a honeypot on the cyber grand challenge final event[J]. IEEE Security & Privacy, 2018, 16(2): 37-41.
- [4] JIA Z P, CUI X, LIU Q X, et al. Micro-Honeypot: using browser fingerprinting to track attackers[C]//2018 IEEE Third Inter-

- national Conference on Data Science in Cyberspace (DSC), June 18-21, 2018, Guangzhou, China. Piscataway: IEEE Press, 2018: 197-204.
- [5] KUMAR S, SEHGAL R, BHATIA J S. Hybrid honeypot framework for malware collection and analysis[C]//2012 IEEE 7th International Conference on Industrial and Information Systems (ICIIS), Aug 6-9, 2012, Chennai, India. Piscataway: IEEE Press, 2012: 1-5.
- [6] CHRISTOS K. Improving mobile core network security with Honeynets[J]. IEEE Security & Privacy, 2007, 5(4): 40-47.
- [7] ZAKARIA W Z, MAKSOM F M, ABDULLAH K. Observing the presence of mobile malwares using low-interaction honeypot[C]//2016 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE), May 30-31, 2016, Batu Feringghi, Malaysia. Piscataway: IEEE Press, 2016: 117-121.
- [8] SONG Y B, ZHU X Y, HONG Y L, et al. A mobile communication honeypot observing system[C]//4th International Conference on Multimedia Information Networking and Security, Nov 2-4, 2012, Nanjing, China. Piscataway: IEEE Press, 2012: 861-865.
- [9] ASIT M, TAPASWI S. A software router based predictive honeypot roaming scheme for network security and attack analysis[C]//9th International Conference of Innovations in Information Technology(IIT), March 17-19, 2013, Paphos, Cyprus. [S.l.:s.n.], 2013: 221-226.
- [10] ELIOT N, KENDALL D, BROCKWAY M. A flexible laboratory environment supporting honeypot deployment for teaching real-world cybersecurity skills[J]. IEEE Access, 2018(6): 34884-34895.
- [11] 邵艾青, 毕喜军, 庞浩. 蜜罐系统与安管平台联动结合的研究与实践[J]. 电信科学, 2017, 33(Z2): 256-261.
- SHAO A Q, BI X J, PANG H. Research and practice of the combination of honeypot system and security management platform[J]. Telecommunications Science, 2017, 33(Z2): 256-261.

[作者简介]



陈利跃 (1973-), 男, 国网浙江省电力有限公司高级工程师、科技信息部信息处处长, 主要研究方向为信息技术。



倪阳旦 (1986-), 男, 国网浙江省电力有限公司工程师, 主要研究方向为网络安全技术和信息技术。



孔晓昀 (1969-), 女, 国网浙江省电力有限公司教授级高级工程师, 主要研究方向为信息技术。

周升 (1985-), 男, 国网浙江省电力有限公司高级工程师, 主要研究方向为网络安全技术。

黄慧 (1983-), 男, 国网浙江省电力公司丽水供电公司高级工程师, 主要研究方向为网络与信息安全。

郑星 (1980-), 男, 国网浙江省电力公司衢州供电公司高级工程师, 主要研究方向为信息系统、安全、信息系统运维、信息化项目建设。