SDN 下基于入侵检测的主动蜜网

严佩敏,姚嘉豪
(上海大学 通信与信息工程学院,上海 200444)

摘　要:提出了一种主动防御技术间的联动方法,通过 SDN(software defined network,软件定义网络)网络和入侵检测系统将未被蜜网欺骗的攻击流量主动迁引至蜜网。该方法主要基于 SDN 网络的可编程性,入侵检测系统根据分析结果自动向 SDN 交换机下发流量的转发策略,实现对攻击流量的主动迁引,完成蜜网对攻击行为的捕获。当访客正常访问时,蜜网系统、入侵检测系统不进行干预,SDN 交换机会将访问流量路由至内网服务器或主机;当存在恶意访问时,蜜网系统作为第一层安全防护,会对恶意访问进行欺骗和诱导;若攻击者未受蜜网欺骗继续攻击内网,入侵检测系统将作为第二层安全防护,会对流向内网服务器的流量进行识别分析,根据分析结果自动生成针对攻击流量的策略指令并下发至 SDN 交换机,将攻击流量主动迁引至蜜网中。

关键词:网络安全;SDN 主动蜜网;流量迁引;入侵检测
中图分类号:TP393　　**文献标识码**:A　　**文章编号**:1673-629X(2021)0096-04

Active Honeynet Based on Intrusion Detection System in Software Defined Network

YAN Pei-min,YAO Jia-hao
(School of Communication and Information Engineering,Shanghai University,Shanghai 200444,China)

Abstract:A linkage method among active defense technologies is proposed,in which the undeceiving attack traffic is actively transferred to the Honeynet through the SDN (software defined network) and intrusion detection system. This method is mainly based on the programmability of SDN,and the intrusion detection system automatically sends the forwarding strategy of the traffic to the SDN switch according to the analysis results,so as to realize the active migration of the attack traffic and complete the Honeynet capture of the attack behavior. When a normal visitor tries to access the server,the switch will route the visitor to intranet servers. If the vistor is a hacker,the Honeynet will work as the first safety protection. If the hacker is not attracted by the Honeynet,the intrusion detection system will work as the second safety protection. By analyzing the flow,the intrusion detection system will automatically generate policy which aims at attack traffic and forward it to switches,then the attack traffic is transferred to Honeynet.

Key words:network security;SDN active Honeynet;flow transfer;intrusion detection

0　引　言

随着互联网技术的飞速发展,针对网络和计算机的攻击也逐渐常态化和复杂化[1],在高度依赖网络的社会环境下,计算机网络安全的重要性日益凸显。目前,解决网络安全问题的方式主要分为被动防御技术和主动防御技术[2],被动防御如防火墙、WAF,主动防御如入侵检测、蜜罐[3]。但这些技术在发展的同时,也存在着功能单一、相互独立、难以管理等不足,不能应对当下逐渐智能化的网络入侵行为。为此,笔者提出一种 SDN 网络下基于入侵检测的主动蜜网模型,通过多种技术的协同工作,提高网络的安全防御能力。

1　相关技术

1.1　入侵检测技术

入侵检测是一种对网络传输进行实时监视,将流量特征与入侵知识库进行匹配,对发现可疑传输时发出警报或者采取主动反应措施的网络安全技术[4]。

入侵检测系统(intrusion detection system,IDS)在检测分析异常行为时,主要分为以下四个阶段:数据收集阶段、数据处理阶段、数据分析阶段、响应处理阶段,如图 1 所示。

在该设计中,入侵检测组件采用开源的 snort,它是在 1998 年由 Martin Roesch 用 C 语言开发的入侵检

收稿日期:2020-12-10
作者简介:严佩敏(1963-),女,博士研究生,副教授,研究方向为智能信息处理、人工智能、数字图像处理、电路系统分析与应用;姚嘉豪(1992-),男,研究方向为计算机网络安全、信息处理。

测系统发展而来[5]。目前已发展成为一个具有多平台、实时流量分析、网络 IP 数据包记录等特性的强大的网络入侵检测系统。

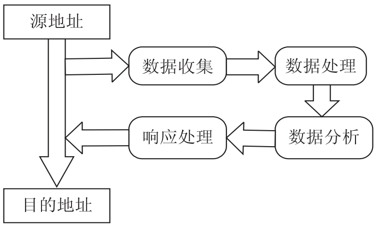

图 1　入侵检测过程

Snort 由以下 4 大软件模块组成:

包嗅探模块:对到达指定网卡的所有流量进行监听;

预处理模块:通过相关插件检查原始数据包,从中发现原始数据的“行为”;

检测模块:依据预先设置的规则数据包对数据包进行检查,一旦发现数据包中的内容和某条规则相匹配,就通知报警模块;

告警/日志模块:网络流量数据若与引擎内的规则相匹配,则触发警报,并记录日志。

Snort 运行方式分为嗅探模式、数据包记录模式、入侵检测模式。在该设计中,Snort 以入侵检测模式(IDS)运行。Snort 对前往目标服务器的所有流量进行监听,与规则库进行比对,若数据包与规则库相匹配,则将告警信息输出至日志。通过脚本程序,抓取告警日志中可疑流量的协议、源目 IP 地址、源目端口等信息,生成流量策略并自动向 SDN 控制器下发指令,实现流量的控制。

1.2　蜜罐技术

蜜网是由多个蜜罐组成的主动安全防御系统[6],一般是由防火墙、路由器以及多台蜜罐主机组成的网络系统。其中蜜罐作为一种诱骗工具,通过设计一个欺骗环境,诱骗攻击者对其进行攻击[7-8],因此任何访问蜜罐的行为都是可疑的,其价值可由其捕获的信息来衡量。

蜜罐又可分为高交互蜜罐和低交互蜜罐。低交互蜜罐基于软件模拟实现,使用资源较少,不容易被利用,但是容易被识别;高交互蜜罐基于真实软硬件构建,真实度高,不容易被识别,但被攻击后,容易被利用,去攻击其他系统,因此风险也比较高。

随着虚拟化技术的进步[9],各种虚拟蜜罐也得到发展,可以通过虚拟机来实现高交互蜜罐,也可以通过 docker 实现业务型蜜罐,比如低交互型 Web 应用蜜罐 Glastopf、中交互 ssh 蜜罐 Cowrie、高交互蜜罐 Emobility 等。其中 docker 轻量化部署的特点,大大提高了蜜罐的灵活性,使用者可以根据实际情况需要,快速部署不同类型的蜜罐,组成混合型蜜网。

1.3　SDN 技术

(software defined network,软件定义网络)是基于软件的一种网络架构,通过将网络设备的控制面和数据转发面分离,从而实现网络流量更灵活的控制,使网络变得更加智能化,是网络虚拟化的一种实现方式[10-12]。其基本架构如图 2 所示。

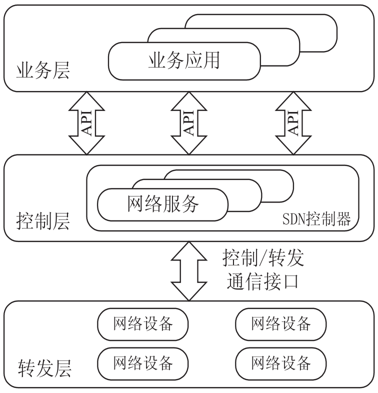

图 2　网络架构

在 SDN 架构中,控制层处在最核心的部分,负责管理整个网络:向上承接应用,可以通过开放 API 接口实现应用层对网络资源的控制;向下对接网络设备,通过标准协议 openflow[14] 与转发层进行通信。该架构特性使用户可以通过编程的方式对所有网络设备进行动态的配置,实现入侵检测系统、蜜罐等安全技术之间的相互协作[15]。

Mininet 是运行在 Linux 环境下的网络仿真平台,它提供了模拟 SDN 网络中的交换机、虚拟主机、控制器和网络链路的方式,并且支持 openflow 协议。在该设计中,SDN 网络环境的搭建,就是基于 mininet 实现。

2　架构设计

为保护企业内部的主机和服务器,使其在遭受攻击后能够尽快恢复,并能够及时对攻击行为进行取证,文中设计了 SDN 网络下基于入侵检测的主动蜜网模型。系统由三个重要组件组成:入侵检测系统、交换机、混合蜜网。

当访客访问服务器时,若访问流量为攻击流量,混合蜜网首先会对攻击流量进行欺骗和诱导;若访客流量未被蜜网欺骗,SDN 交换机会将流量镜像至入侵检测系统进行分析检测,若未匹配检测规则库,入侵检测系统不做任何处理,SDN 交换机正常转发流量,访客可正常访问内网服务器;若与检测规则库匹配,则入侵检测系统会根据可疑流量的特征信息生成流表策略,自动下发至 SDN 交换机,将可疑流量迁引至混合蜜网进行进一步分析,如图 3 所示。

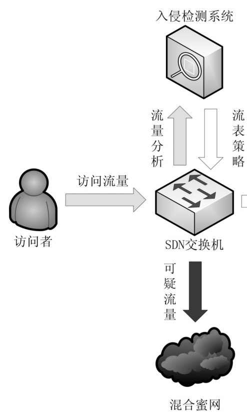

图 3　访问服务器示意图

3　实验验证

为测试文中提出的主动蜜网模型安全防御有效性,使用 mininet 仿真模拟器搭建了小型网络环境,将混合蜜网和入侵检测系统通过 SDN 交换机互联,对目标主机进行攻击,检测蜜罐是否捕获到攻击信息。具体步骤如下:

(1)查看当前蜜网捕获情况,清除目标主机的相关日志;

(2)配置入侵检测日志输出方式为 csv 格式,输出内容包括流量说明、源地址、源端口、目的地址、目的端口、协议,如图 4 所示;

```
###################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
###################################################
output alert_csv: /home/yaojiahao/msglog.csv msg,proto,src,srcport,dst,dstport
```

图 4　日志输出方式及输出内容

(3)配置入侵检测策略,当检测到所有目的地址为 192.168.1.89 的流量发出告警,写入日志,如图 5 和图 6 所示;

```
#-------------
# LOCAL RULES
#-------------

#NMAP Ping扫描检测:
#alert icmp any any -> 192.168.1.89 any (msg: "Nmap ICMP Scan"; dsize:0;sid:10000004; rev: 1; )
```

图 5　入侵检测策略

```
"attack from Internet!",TCP,194.26.29.123,59492,192.168.1.89,44881
"attack from Internet!",TCP,194.26.29.146,52309,192.168.1.89,50060
"attack from Internet!",TCP,93.88.74.232,58081,192.168.1.89,10569
"attack from Internet!",TCP,194.26.29.134,40288,192.168.1.89,2441
"attack from Internet!",TCP,195.54.166.157,56082,192.168.1.89,5318
"attack from Internet!",TCP,193.106.30.226,43274,192.168.1.89,3388
"attack from Internet!",TCP,149.28.119.209,57009,192.168.1.89,22
```

图 6　告警日志

(4)Snort 根据日志中的相关信息生成流表策略,通过定时任务将指令下发至 SDN 交换机,实现流量迁引,如图 7 和图 8 所示;

```
nw_src=194.26.29.137,nw_dst=192.168.1.89,actions=output:2
ovs-ofctl add-flow s1 dl_type=0x0800,priority=200,idle_timeout=600,hard_timeout=300,
nw_src=194.26.29.123,nw_dst=192.168.1.89,actions=output:2
ovs-ofctl add-flow s1 dl_type=0x0800,priority=200,idle_timeout=600,hard_timeout=300,
nw_src=194.26.29.146,nw_dst=192.168.1.89,actions=output:2
ovs-ofctl add-flow s1 dl_type=0x0800,priority=200,idle_timeout=600,hard_timeout=300,
nw_src=93.88.74.232,nw_dst=192.168.1.89,actions=output:2
ovs-ofctl add-flow s1 dl_type=0x0800,priority=200,idle_timeout=600,hard_timeout=300,
nw_src=194.26.29.134,nw_dst=192.168.1.89,actions=output:2
ovs-ofctl add-flow s1 dl_type=0x0800,priority=200,idle_timeout=600,hard_timeout=300,
nw_src=195.54.166.157,nw_dst=192.168.1.89,actions=output:2
ovs-ofctl add-flow s1 dl_type=0x0800,priority=200,idle_timeout=600,hard_timeout=300,
nw_src=193.106.30.226,nw_dst=192.168.1.89,actions=output:2
ovs-ofctl add-flow s1 dl_type=0x0800,priority=200,idle_timeout=600,hard_timeout=300,
nw_src=149.28.119.209,nw_dst=192.168.1.89,actions=output:2
```

图 7　流量策略生成

```
NXST_FLOW reply (xid=0x4):
 cookie=0x2a00000000000004, duration=56.962s, table=0, n_packets=3, n_bytes=238, idle_
timeout=600, hard_timeout=300, idle_age=52, priority=10,dl_src=8a:d1:59:61:59:c2,dl_ds
t=42:f8:04:a5:65:b9 actions=output:4
 cookie=0x2a00000000000005, duration=56.962s, table=0, n_packets=3, n_bytes=238, idle_
timeout=600, hard_timeout=300, idle_age=52, priority=10,dl_src=42:f8:04:a5:65:b9,dl_ds
t=8a:d1:59:61:59:c2 actions=output:3
 cookie=0x0, duration=7.69s, table=0, n_packets=0, n_bytes=0, idle_timeout=600, hard_t
imeout=300, idle_age=7, priority=200,ip,nw_src=193.106.30.226,nw_dst=192.168.1.89 acti
ons=output:2
 cookie=0x0, duration=7.696s, table=0, n_packets=0, n_bytes=0, idle_timeout=600, hard_
timeout=300, idle_age=7, priority=200,ip,nw_src=195.54.166.157,nw_dst=192.168.1.89 act
ions=output:2
 cookie=0x0, duration=9.812s, table=0, n_packets=0, n_bytes=0, idle_timeout=600, hard_
timeout=300, idle_age=9, priority=200,ip,nw_src=194.26.29.123,nw_dst=192.168.1.89 acti
ons=output:2
 cookie=0x0, duration=7.678s, table=0, n_packets=0, n_bytes=0, idle_timeout=600, hard_
timeout=300, idle_age=7, priority=200,ip,nw_src=149.28.119.209,nw_dst=192.168.1.89 act
ions=output:2
 cookie=0x0, duration=7.752s, table=0, n_packets=0, n_bytes=0, idle_timeout=600, hard_
timeout=300, idle_age=7, priority=200,ip,nw_src=194.26.29.134,nw_dst=192.168.1.89 acti
ons=output:2
 cookie=0x0, duration=7.774s, table=0, n_packets=0, n_bytes=0, idle_timeout=600, hard_
timeout=300, idle_age=7, priority=200,ip,nw_src=93.88.74.232,nw_dst=192.168.1.89 actio
ns=output:2
 cookie=0x0, duration=8.297s, table=0, n_packets=0, n_bytes=0, idle_timeout=600, hard_
timeout=300, idle_age=8, priority=200,ip,nw_src=194.26.29.146,nw_dst=192.168.1.89 acti
ons=output:2
 cookie=0x2b00000000000007, duration=58.068s, table=0, n_packets=3, n_bytes=238, idle_
age=57, priority=2,in_port=3 actions=output:2,output:1,output:4,CONTROLLER:65535
 cookie=0x2b00000000000005, duration=58.068s, table=0, n_packets=577576, n_bytes=55661
4294, idle_age=0, priority=2,in_port=1 actions=output:2,output:4,output:3,CONTROLLER:6
5535
 cookie=0x2b00000000000006, duration=58.068s, table=0, n_packets=3, n_bytes=238, idle_
age=57, priority=2,in_port=4 actions=output:2,output:1,output:3,CONTROLLER:65535
 cookie=0x2b00000000000004, duration=58.072s, table=0, n_packets=36, n_bytes=8550, idl
e_age=2, priority=2,in_port=2 actions=output:1,output:4,output:3,CONTROLLER:65535
 cookie=0x2b00000000000001, duration=60.039s, table=0, n_packets=12, n_bytes=1917, idl
e_age=11, priority=100,dl_type=0x88cc actions=CONTROLLER:65535
 cookie=0x2b00000000000001, duration=60.009s, table=0, n_packets=1569, n_bytes=1623171
5, idle_age=58, priority=0 actions=drop
```

图 8　指令下发成功

(5)查看蜜网捕获到的攻击信息,与入侵检测告警日志进行比对,如图 9 所示。


```
dest_ip: 192.168.1.89 t-pot_ip_ext: 139.227.59.222 t-pot_hostname: grievingbrief params: none host: fe77d1cde93a geoip.dma_code: 511 geoip
geoip.latitude: 39.001 geoip.timezone: America/New_York geoip.city_name: College Park geoip.region_name: Maryland geoip.location: { "lon":
geoip.postal_code: 20740 geoip.ip: 149.28.119.209 geoip.country_code2: US geoip.country_name: United States geoip.longitude: -76.932 geoip.
geoip.country_code3: US tags: _geoip_lookup_failure t-pot_ip_int: 192.168.1.76 type: P0f subject: cli os: ??? dist: 13 @timestamp: May 9t
raw_sig: 4:242+13:0:0:65535,0:::0 src_port: 57009 path: /data/p0f/log/p0f.json mod: syn @version: 1 src_ip: 149.28.119.209 _id: NgL3-HEB56

dest_ip: 192.168.1.89 t-pot_ip_ext: 139.227.59.222 t-pot_hostname: grievingbrief params: tos:0x08 host: fe77d1cde93a tags: _geoip_lookup_fa
type: P0f subject: cli os: ??? dist: 16 @timestamp: May 9th 2020, 18:25:02.000 dest_port: 5318 raw_sig: 4:239+16:0:0:1024,0:::0 src_port:
path: /data/p0f/log/p0f.json mod: syn @version: 1 src_ip: 195.54.166.157 _id: KQL3-HEB568IWofihNjO _type: doc _index: logstash-2020.05.09

dest_ip: 192.168.1.89 t-pot_ip_ext: 139.227.59.222 t-pot_hostname: grievingbrief params: none host: fe77d1cde93a tags: _geoip_lookup_failur
type: P0f subject: cli os: ??? dist: 13 @timestamp: May 9th 2020, 18:25:02.000 dest_port: 2441 raw_sig: 4:242+13:0:0:1024,0:::0 src_port:
path: /data/p0f/log/p0f.json mod: syn @version: 1 src_ip: 194.26.29.134 _id: KgL3-HEB568IWofihNjS _type: doc _index: logstash-2020.05.09

dest_ip: 192.168.1.89 t-pot_ip_ext: 139.227.59.222 t-pot_hostname: grievingbrief params: none host: fe77d1cde93a geoip.region_code: ZH geo
geoip.timezone: Europe/Amsterdam geoip.city_name: Naaldwijk geoip.region_name: South Holland geoip.location: { "lon": 4.216, "lat": 51.9934
geoip.as_org: WorldStream B.V. geoip.ip: 93.88.74.232 geoip.country_code2: NL geoip.country_name: Netherlands geoip.longitude: 4.216 geoip.
geoip.asn: 49981 geoip.country_code3: NL t-pot_ip_int: 192.168.1.76 type: P0f subject: cli os: ??? dist: 17 @timestamp: May 9th 2020, 18:
raw_sig: 4:238+17:0:0:1024,0:::0 src_port: 58081 path: /data/p0f/log/p0f.json mod: syn @version: 1 src_ip: 93.88.74.232 _id: KwL3-HEB568I

dest_ip: 192.168.1.89 t-pot_ip_ext: 139.227.59.222 t-pot_hostname: grievingbrief params: none host: fe77d1cde93a geoip.latitude: 50.45 geo
"lat": 50.45 } geoip.longitude: 30.523 geoip.continent_code: EU geoip.as_org: Infium, UAB geoip.ip: 193.106.30.226 geoip.country_code2: UA
geoip.country_name: Ukraine geoip.country_code3: UA t-pot_ip_int: 192.168.1.76 type: P0f subject: cli os: ??? dist: 17 @timestamp: May 9t
dest_port: 3388 raw_sig: 4:238+17:0:0:1024,0:::0 src_port: 43274 path: /data/p0f/log/p0f.json mod: syn @version: 1 src_ip: 193.106.30.226
_type: doc _index: logstash-2020.05.09 _score: -
```


图 9　蜜网收集到的攻击信息

通过实验结果可以看出,该模型可有效实现入侵检测系统自动生成流表策略并下发至 SDN 交换机,对攻击流量进行迁引的功能。与传统蜜网相比,更具有主动性,安全防护系统整体更加智能化。

4　结束语

针对当前各类安全防护系统功能单一、相互独立、难以管理的问题,设计了将入侵检测系统、网络、混合蜜网相互结合的智能蜜网模型。在混合蜜网高欺骗性的基础上,基于网络可编程特性,通过入侵检测系统自动向交换机下发指令,将未受蜜网欺骗的攻击流量进行迁引,实现第二层安全防护,大幅提升了安全防护能力;同时通过蜜网捕获的信息,可以对攻击链进行追溯还原。最后,通过模拟实验,验证了模型的可行性和有效性。

参考文献:

[1] RIDEN J, MCGEEHAN R, ENGERT B, et al. Know your enemy: Web application threats, using honeypots to learn about HTTP - based attacks [EB/OL]. 2011. http://honeynet. onofri. org/papers/webapp/.

[2] 曹爱娟,刘宝旭,许榕生. 网络陷阱与诱捕防御技术综述[J]. 计算机工程,2004,30(9):1-3.

[3] 彭　珺,高　珺. 计算机网络信息安全及防护策略研究[J]. 计算机与数字工程,2011,39(1):121-124.

[4] 胡华平,陈海涛,黄辰林,等. 入侵检测系统研究现状及发展趋势[J]. 计算机工程与科学,2001,23(2):20-25.

[5] 李晓芳,姚　远. 入侵检测工具 Snort 的研究与使用[J]. 计算机应用与软件,2006,23(3):124-141.

[6] 王　璐,秦志光. 业务蜜网技术与应用[J]. 计算机应用,2004,24(3):43-45.

[7] 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.

[8] 程杰仁,殷建平,刘　运,等. 蜜罐及蜜网技术研究进展[J]. 计算机研究与发展,2008,45(增刊):375-378.

[9] 项国富,金　海,邹德清,等. 基于虚拟化的安全监控[J]. 软件学报,2012,23(8):2173-2187.

[10] 张朝昆,崔　勇,唐翯翯,等. 软件定义网络(SDN)研究进展[J]. 软件学报,2015,26(1):62-81.

[11] 左青云,陈　鸣,赵广松,等. 基于 OpenFlow 的 SDN 技术研究[J]. 软件学报,2013,24(5):1078-1097.

[12] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow: enabling innovation in campus networks[J]. ACM SIGCOMM CCR,2008,38(2):69-74.

[13] MIT Technology Review. 10 breakthrough technologies, TR10: software-defined networking[EB/OL]. 2009. http://www2. technologyreview. com/article/412194/tr10 - software-defined-networking.

[14] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow: enabling innovation in campus networks[J]. SIGCOMM Computer Communication Review, 2008, 38(2):69-74.

[15] 陆腾飞. 面向蜜场环境的网络攻击迁移技术的研究与实现[D]. 北京:北京大学,2009.