Implementing Lightweight Intrusion Detection Systems Based on Network Function Virtualization

Nikhil Vijayakumar Kengalahalli
nikhilvijayakumar.kengalahalli@sjsu.edu
Suhas Janardhan
suhas.janardhan@sjsu.edu
Younghee Park
younghee.park@sjsu.edu
San Jose State University
San Jose, CA 95192

Abstract - The advent of Network Function Virtualization (NFV) has provided high scalability and flexibility in developing intrusion detection systems while replacing the deployment of hardware middleboxes with software-based network appliances. This paper introduces a method of implementing intrusion detection systems (IDS) based on the concept of NFV by using ClickOS, an open source NFV project. According to, NFV enables students to develop intrusion detection systems to detect various network attack types utilizing very few computing resources. The survey results showed that students can easily understand the specific attacks and implement their own small IDS based on ClickOS.

Keywords

Network Function Virtualization, Intrusion Detection Systems, ClickOS, Network Security

1. INTRODUCTION

The emerging technology of Network Function Virtualization(NFV) has dramatically transformed the nature of core network middleboxes, such as Intrusion Detection System, Network Address Translators, Firewalls, providing software-based network appliances on virtualization. NFV enables decoupling of network functions from dedicated hardware into software instances running on commodity servers [1]. It provides programmability, scalability, and, management and orchestration of networks to effectively defend against various network attacks.

Recent research has proposed security appliances based on NFV to defend against various network attacks. VNGuard implemented an NFV-based Firewall [1], and Bohatei [4] has provided a scalable DDoS attack detection system using NFV and SDN (software defined networking). In addition, SHIELD [5] has proposed a security framework to provide various security services based on NFV. A machine-learning-based threat detection system on NFV was presented to defend against real-time network threats. However, in spite of advanced NFV network detection systems, educational materials are lacking for students to learn how to develop security functions on NFV.

In this paper, we introduce NFV-based security education materials to help any user to develop their own intrusion detection function based on NFV. It includes information about the NFV concept, instructions on developing each function, and indicates the purpose which each proposed function serves. Initially, we provided three sample security lab exercises and explained the relationship of each lab and security issues. The basic security labs covered a network function related to deep packet inspection, ICMP Ping detection, and TCP SYN Flooding detection. We also conducted a user survey to evaluate the effectiveness and the usability of each security lab. As a result, students showed a high level of interest in developing their own intrusion detection system based on NFV.

The rest of the paper will be as follows: Section 2 will show related work in NFV, especially in security; Section 3 will introduce our security labs and then we will evaluate our labs in Section 4. We will discuss our work in Section 5 and our conclusion is in Section 6.

2. RELATED WORK

Network Function Virtualization is a new network technology to virtualize hardware network appliances in order to reduce operation and maintenance costs while providing flexibility, scalability and programmability in networks. ClickOS is an open source software to create flexible routers with virtualization to achieve NFV technology [3]. Because of the advantages of Network Function Virtualization, new security defense systems have been proposed to protect networks [1, 2, 4, 5]. VNGuard [1] developed a virtual firewall to safeguard networks by separating the firewall from the dedicated hardware. Bohatei [4] developed a flexible and scalable defense method against various network DDoS attacks by using NFV and SDN (Software Defined Networking). SHIELD[5] provided a sophisticated cyber security framework, offering security-as-a-service. In addition, to achieve micro-services based on NFV, some research has focused on developing a monolithic network function design to modularize each intrusion detection function in NFV to replace a single complicated IDS [2]. Such a design offers more scalability and flexibility to manage various attack types while reducing CPU usage and processing power.

3. INTRUSION DETECTION SYSTEM BASED ON NFV

Network intrusion detection systems (NIDS) discover unauthorized access to certain network resources by analyzing network traffic for signs of malicious activities that could undermine the normal operation of a network. They have been proved to be effective in defending against traditional cyber threats by combining various attack analysis techniques with other systems like firewalls and penetration testing systems. There

has been no standard development platform to design NIDS. However, using ClickOS to achieve NFV, we now are able to design and develop many specific intrusion detection network functions because of the easy design and simple deployable network functions provided by ClickOS for NFV. Using ClickOS changes the IDS development paradigm.

2.1 Sample Security Labs based on ClickOS

ClikOS is an open source platform to achieve software routers based on NFV by using Xen hypervisor [7]. ClikOS consists of various packet processing functions, called click elements. There are a lot of click elements to implement various flexible router functions, such as packet classification, queuing, and scheduling. It supports various network protocols including Ethernet, IP, TCP and UDP, which provide basic network functions. Based on the open source platform, students can implement their own IDS to detect attacks. Three examples of labs that can be used to create an independent intrusion detection function or as a component in another IDS are: (1) Packet Content Inspection, (2) ICMP Ping Detector, and (3) TCY SYN Flooding Detector.

Figure 1 shows the Xen configuration file to make a click file run in ClickOS on a single machine. We distributed this Xen configuration file to our students to allow them to do each lab by simply assigning their own click file name (i.e. tcpsyn.click) in the last line of the configuration file. In the configuration file, the *name* refers to the user domain of the ClickOS instance and the *kernel* indicates the location of the ClickOS binary file. The *vcpus* is the number of virtual CPUs. The *vif* refers to the virtual interface where ClickOS would attach. Lastly, the *click* refers to a click application (i.e. tcpsyn.click) which gets executed when the ClickOS instance is started.

Figure 1. A Xen configuration file

(1) Security Lab 1: Packet Content Inspection

This lab enables students to look at packet contents for further attack investigation, which is an important network intrusion detection function for deep packet inspection (DPI) [9]. DPI is used to identify attack signatures in the payload of incoming or outgoing packets in a router. The first lab will take the first step in student ability to develop a complete DPI function based on ClickOS.

To print packet contents, we use three main click elements: *FromDevice*, *ToDevice*, and *EtherMirror*. The first click application includes only "*FromDevice -> Print ('OK') -> EtherMirror -> ToDevice*." The *FromDevice* click element reads the packet from a network device and then directs it to the *Print* click element, which prints the contents of packets along with the label 'OK,' which is provided as a parameter. Then it is directed to the *EtherMirror* click element, which swaps the Ethernet source and destination. Finally, it is sent to the *ToDevice* click element, which sends the packet to the network device, which is the source that has been swapped with the previous destination by the swapping click element, *EtherMirror*. Figure 2 shows the results of this click file on ClickOS. With this click file, users can link this click file with an extra virus signature-matching program to detect viruses in the payload.

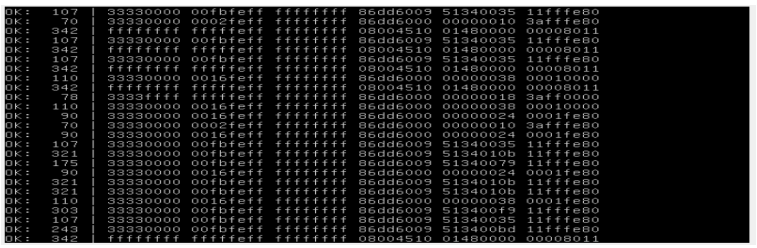

Figure 2. The results from the click file used to print the packet payload.

(2) Security Lab 2: Ping Flooding Attack Detection

The Ping flooding attack is an ICMP-based denial-of-service (DoS) attack that floods a high volume of ICMP request (ping) packets to a targeted machine in order to saturate incoming and outgoing bandwidth at the victim machine [8]. To detect this ping flooding attack, we can implement a detection click application based on ClickOS. Figure 3 shows an example of the Ping flooding attack detection. In a Ping flooding attack detection, we first assign an IP address and its Mac address to the click application in Figure 3. This click application classifies incoming packets into ARP requests or IP packets. All ARP request packets are directed to the *ARPPrint* click element and then to the *ARPResponder* click element to generate ARP responses for the destination. Similarly, for all IP packets, ICMP echo replies are sent to the final destination through *EtherMirror* after printing the echo packets. In the process of capturing the IP packets, the *TCounter* element keeps counting the number of echo request packets. If the number of echo packets exceeds a certain threshold, this click application raises an alert for the Ping flooding attack. All packets other than APR requests and IP packets are discarded. Figure 4 demonstrates that the designed click application was able to detect Ping flooding attacks.

The *TCounter* is a new element that we implemented in ClickOS. We are able to set a threshold in the *TCounter* click element. When the number of SYN packets exceeds that designated threshold, our click application sends an alert message to the system. A detailed explanation of how to add

a new element in ClickOS is beyond the scope of this paper. Users can simply utilize a new click element, which is another benefit of ClickOS.

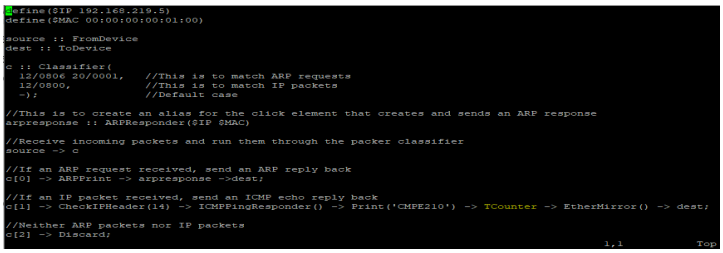

Figure 3. A click application for Ping flooding attack detection

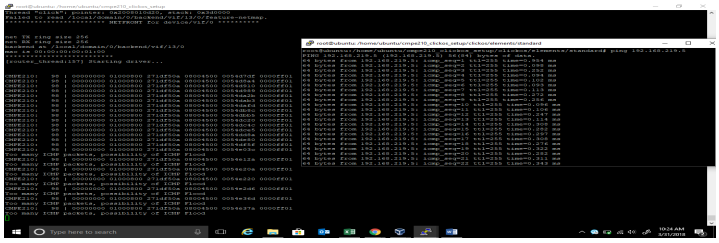

Figure 4. The results of Ping flooding detection

(3) Security Lab 3: TCP SYN Flooding Attack Detection

TCP SYN flooding attacks are the most frequent DoS attacks in which attackers send a lot of SYN packets to establish connections between clients and servers. Because of the overwhelming number of requests, the server exhausts the resource and cannot respond to further legitimate requests. To defend against these SYN flooding attacks, many defense methods have been proposed by various research communities [8]. Figure 5 shows a click application to detect SYN flooding attacks using ClickOS. To accomplish this, we first specified an IP address and its MAC address to this click application. The incoming packets were classified using the *Classifier* to identify only the TCP SYN packets. Only the TCP packets were stripped of header details and then passed on to the *TCounter* element, which then counted only the number of SYN packets.

We then set the threshold for the *TCounter* so that when the number of SYN packets exceeded that threshold, our click application would give an alert message to the system. Figure 6 demonstrates the results of this click application, which detected SYN flooding attacks when the threshold of the *TCounter* was set at 20. It is a lightweight intrusion detection function with virtualization to detect TCY SYN flooding attacks. Users can implement their own similar intrusion detection functions, such as HTTP flooding attacks and UDP flooding attacks. Users can combine all the intrusion detection functions into a complete IDS with virtualization or utilize a single virtualized function to target a specific attack.

```
define($IP 192.168.56.105)
define($MAC 00:00:00:00:01:00)

source :: FromDevice
dest :: ToDevice

c :: Classifier(
  23/06,            //This is to match TCP SYN packets
  -);                 //Default case

source -> c

c[0] -> Strip(26) -> Print('TCP Packet', 0) -> TCounter -> EtherMirror -> dest;
c[1] -> Print('OTHERS',0)  -> Discard;
```

Figure 5. A click application for TCP SYN flooding attack detection

```
TCP Packet:  28
Flag Value: 02
TCP Packet:  28
Flag Value: 02
TCP Packet:  28
Flag Value: 02
Too many SYN packets, possibility of TCP SYN Flood
TCP Packet:  28
Flag Value: 02
Too many SYN packets, possibility of TCP SYN Flood
TCP Packet:  28
Flag Value: 02
Too many SYN packets, possibility of TCP SYN Flood
TCP Packet:  28
Flag Value: 02
Too many SYN packets, possibility of TCP SYN Flood
TCP Packet:  28
```

Figure 6. The results of the TCP SYN flooding attack detection click application

4. EVALUATION

We evaluated our three labs in the current SDN/NFV class in Computer Engineering at San Jose State University, explaining security concepts for each lab. There were thirty students who had never previously been introduced to SDN or NFV. They finished these three labs and responded to a user survey. The user survey aimed to evaluate the lab's usability, its usefulness in understanding security problems, and student interest in designing more security functions in ClickOS. The survey items measured the degree to which students agreed or disagreed with the following: (Q1) Students can understand each security problem through these labs; (Q2) The lab materials help students to implement

their own intrusion detection functions in ClickOS; (Q3) The lab contents are clear and easy to follow; (Q4) The labs are helpful to understand IDS using NFV; (Q5) Students who did the lab will study another security problem and develop a new intrusion detection function in ClickOS; and (Q6) Students who did the lab will be interested in studying NFV after these labs.

Figure 7 shows the results of the student survey. More than 50% of the students provided positive feedback on the labs. Around 66% of the students thought that the labs helped them to understand a security problem and to implement a new intrusion detection function. Around 86% of the students agreed that the lab materials were clear and easy to follow, suggesting that they were well-designed with effective instructions. Furthermore, more than 80% of the students thought the labs created more interest in students wanting to study NFV and developing their own IDS in ClickOS. We also asked for student feedback about the labs. Although the students viewed the labs positively, most of the students indicated that they made some mistakes in setting up the ClickOS environment since they were not familiar with virtualization techniques.

Network Function Virtualization enables students to develop lightweight network functions which dynamically spawn instances with virtualization. It separates network functions from physical fixed locations in the middleboxes and provides high scalability and efficiency to be deployed throughout a network. Thus, the development of IDS should utilize these advantages of NFV to produce a scalable and platform independent IDS for the future. To maximize the usage of such emerging technologies, educational materials in NFV are of great importance to encourage users to implement a new IDS in NFV. ClickOS provides an open platform to initiate this new paradigm for NFV.

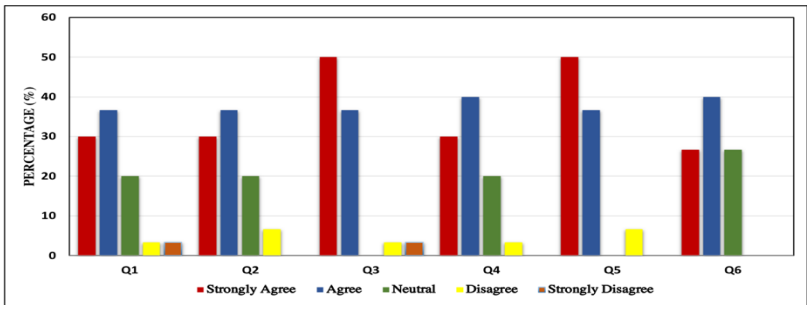

Figure 7. The results of the user survey for the three labs

5. CONCLUSION

This paper provides basic educational materials to help students to develop a simple intrusion detection system in NFV. Based on the open source project, ClickOS, we proposed three different security labs that can be used as fundamental resources to enable users to develop a complete IDS in ClickOS to achieve a new IDS in NFV. We performed the survey after asking students to finish these three labs in our SDN/NFV class at San Jose State University. As a result, students showed interest in developing other intrusion detection functions in ClickOS and to continue to learn about NFV. For future work, we will create many intrusion detection functions in ClickOS to help students to understand various security problems and develop defense methods using ClickOS.

Acknowledgment

This work is supported by NSF SaTC #1723804.
Dr.Park is a corresponding author.

REFERENCES

[1] J. Deng et al., "VNGuard: An NFV/SDN combination framework for provisioning and managing virtual firewalls," 2015 IEEE Conference on Network Function Virtualization and Software Defined Network (NFV-

SDN), San Francisco, CA, 2015, pp. 107-114. doi: 10.1109/NFV-SDN.2015.7387414

[2] Y. Park, P. Chandaliya, A. Muralidharan, N. Kumar et al., “Dynamic Defense Provision via Network Functions Virtualization,” ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization, pp. 43-46, 2017

[3] J. Martins, M. Ahmed, C. Raiciu, V. Olteanu, and M. Honda, “ClickOS and the Art of Network Function Virtualization,” USENIX Symposium on Networked Systems Design and Implementation (NSDI), 2014

[4] Y. Tobioka, V. Sekar et al., “Bohatei: Flexible and Elastic DDoS Defense,” USENIX Security Symposium, 2015

[5] G. Gardikis et al., "SHIELD: A novel NFV-based cybersecurity framework," 2017 IEEE Conference on Network Softwarization (NetSoft), Bologna, 2017, pp. 1-6. doi: 10.1109/NETSOFT.2017.8004228

[6] M. A. Lopez, A. G. P. Lobato, O. C. M. B. Duarte and G. Pujolle, "An evaluation of a virtual network function for real-time threat detection using stream processing," 2018 Fourth International Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 2018, pp. 1-5. doi: 10.1109/MOBISECSERV.2018.8311440

[7] Joao Martins, Mohamed Ahmed, Costin Raiciu, Vladimir Olteanu, et. al., “ClickOS and the Art of Network Function Virtualization,” 11th USENIX Symposium on Networked Systems Design and Implementation (NSDI), Seattle, WA, USA 2014.

[8] CERT Advisory, “TCP SYN Flooding and IP Spoofing Attacks,” in Advisory, Software Engineering Institute, Carnegie-Mellon University, 1996.

[9] Thaksen J. Parvat, Pravin Chandra, “A Novel Approach to Deep Packet Inspection for Intrusion Detection,” Elsevier Journal of Procedia Computer Science, Volume 45, Pages 506-513, ISSN 1877-0509, 2015.