VCSL: A Virtual Cyber Security Lab

Sachin P C*, Harsh Bhojani†
Computer Science & Information Systems, Birla Insitute of Technology & Science, Pilani, IND.
Email: *h20180140@pilani.bits-pilani.ac.in, †h20180125@pilani.bits-pilani.ac.in

***Abstract*—In today's world, computer network attacks are brought out by professionals targeting groups vulnerabilities. Several interventions are thriving because of the increasing complexity of unprotected data technology lacking care. since appears as no wonder that "cyber-security" protection resolutions on suggestion are growing exponentially. Consequently, learning the function of these explications in the circumstances of how they are used claims network-administrators of the future to have the in-detail experience, knowledge, and working practice. We demonstrate the design and prototype of virtual cyber security lab. By building this lab we can better understand the network security tools, analyze the network and exploit the vulnerabilities present which can cause security threats. The main objective is to gain the practical knowledge in the domain of network security and to perform attacks on network, respond to threats.**

***Index Terms*—vulnerabilities, interventions, virtual cyber-security lab, explications, network-administrators, attacks, threats.**

I. INTRODUCTION

"TODAY anybody who is able to spell the word security immediately gets a well-paid job," said Dr. William Simpson from the Institute of Defense Analyses, USA, during the 7th International Conference on Complexity, Informatics and Cybernetics, IMCIC 2016, held in Orlando, March 2016. All in all, easier said than done.The security notions of organizations and companies, no extent they are, has to be "all-encompassing". It involves the security of information, adjacent with each transmission carrier and a network element. A security-manager, therefore, requires to be a security expert proper than an IT-graduate with comprehensive training. He/she requires to be in a place to effectively addressed demands placed security without spending a huge amount of time in obtaining new crafts and new understanding of IT security. Moreover, attacks exposed every day by the media, and the powerful connection of every kind of companies on IT is letting the need for safety authorities to stimulate dramatically. long-time ago that IT security was totally underrated, not only judgment makers in organizations, state-owned and private corporations but also in universities. Increasingly, though, people have appeared to recognize the unique risks of cyber attacks. The annual disaster goes into a huge amount.

A laboratory is as important to a computer-security specialist as it is to a chemist or biologist and network security, is a field in which the researcher must understand how a diverse range of technologies behaves at many levels. Determine the necessary network security tools needed to safeguard any organization. Conventional methods of schooling (i.e. lectures or books) have become to be not satisfactory for cyber-security practice because the trainee cannot implement the policies from the academic procedure to practical circumstances during the course. Vulnerability exercise, achieving hands-on practice by exercises is essential for combining knowledge. Besides this, just realistic training is becoming to efficiently explain the significance of details: a small hole in a service or firewall configuration may demolish all attempts to secure a system or network.

Specifically, the allotment of an environment for these useful training settings acts as a test not only for teachers but also for analysis and improvement. That is because students require "privileged access rights" (root/administrator) on the testing method to run utmost the possible security actions. By those rights, pupils might quickly destroy a practice system or even use it for unintended, unauthorized attacks on other hosts on the university network or the Internet world. Conventional means for effective cyber-security education are committed, separated network-labs for security training. These labs are costly and requiring making and maintenance. Primarily for the testing of network-security topics, an individual student requires a workplace with many networked computers. Due to the drawbacks, there is a trend towards the provision of such laboratories using virtual machine technology.Because there is no one size fits all solution to network security, the Introduction to Network Security Tools Virtual Lab will prepare you with a basic knowledge about which tool is best based on your security strategy. It is also provides work environments and basic cyber facilities for project.

II. SETTING UP A VIRTUAL LAB

setting Here, we have mostly focus on two major concepts where:

- one we have implemented a virtual lab with $single - system.$
- other with two or more means with $mulitple - systems.$

The detail explanation of these concepts as follows:

1) **A virtual lab with single system:** In this, we have implemented a entire virtual lab using only single host. we have used $virtualbox$ to make different nodes(PCs) and an open-source router distribution knows as $PfSense$ to implement and configure the routers and firewalls. As given in the above diagram, you can see that the entire virtual lab is there within the single machine. Here, we have three ubuntu machines all are having different subnet mask means all these three are in different networks. in which one system is $kali - linux$(PC-1) and other two are $ubuntu - 16.04$(PC-2) and we

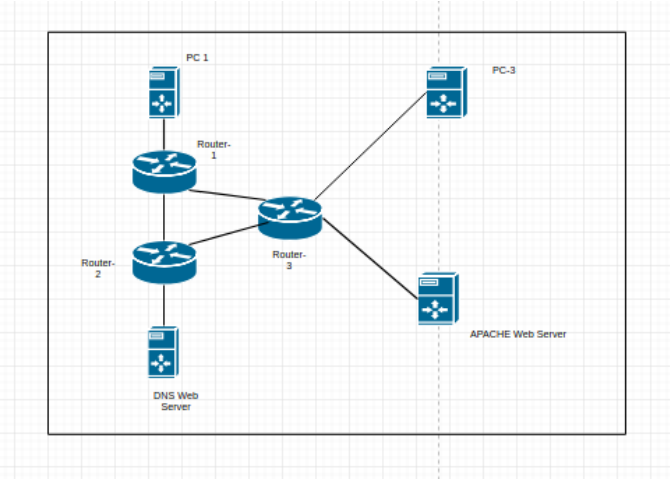

Fig. 1. VCSL using single-system

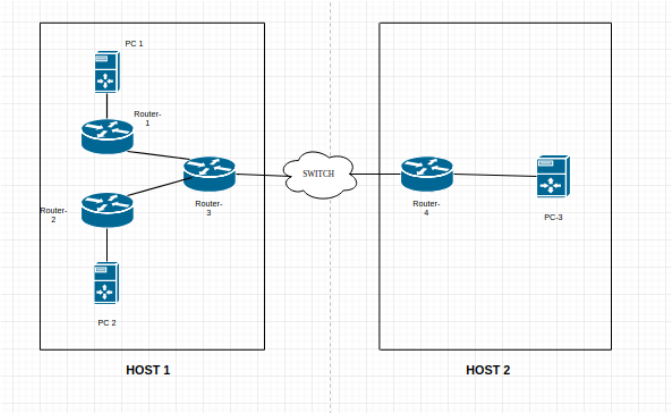

Fig. 2. VCSL using two-system

have configure the system connected to router $R1$ as DNS server using $bind9 - utility$ we also planning to make one more system as DNS client in the future to perform the DOS kinda attack. we will also have one more system on which we have configured the $web - server$(PC-3) which will give the effect of "the outer-world"(Internet in some sense) connected to router $R2$. all the routers are configured in such way that will transfer the packet as expected. Here, entire topology is having internal-network interface so that there is no communication to actual outside world(other then this network).

2) **A virtual lab with two systems:** In this, we have implemented a virtual lab with the use of two systems. where we have connected hots with the use of switch and then in one host we have configured the two network as given in the figure and on the other host we have one web-server so here the outer-world effect is given by the second host. Here, in the first host we have router $R1$ and $R2$ connected two different subnet(networks) and also having the same topology which is given in the first approach(with single system). while, in second host we are having one router $R3$ which is connected to the PC which having $liunx$ operating system running on it and also configured as a "web-server". Here, both these host are given static-IP addresses so that they can transfer the network packets without having any trouble. All the routers are configured in such way that will transfer the packet as expected. here entire topology is having internal-network interface so that there is no communication to actual outside world(other then this network).

III. INSTALLATION

In this, we will explain the steps to install virtual box in Ubuntu. Open your terminal by pressing control alt T.The enter the following commands in order:

```
$ sudo apt-get update
$ sudo apt-get upgrade
$ sudo apt-get update
$ sudo apt-get install virtualbox -5.2
```

Once everything is done , you can turn on the virtual box by typing "Virtualbox" in commmand line terminal.

Once, virtual box is up and running, you can add any number of host machines depending on the system in which you are running the virtual box. To install Linux Ubuntu machine in virtual box,

1) Download the Ubuntu ISO file from their website.
2) Click on the new option available in the virtual box.
3) Give the memory required and the hard disk storage for the system and add the ISO fileby clicking on the storage.
4) Now, start the machine and give all default values and then install the linux machine.

- **Installation of the router using pfsense:** once the host machines are setup, now to create a virtual network, we need to install the routers. The following are the steps to install the router in the virtual box:
  1) downloading a BSD ISO file from the pfsense official website.
  2) Once downloaded, click on the new button in the virtual box.
  3) Enter the details like given below in the pictures and then click next
  4) Now, give all the default configurations and add the ISO file in the storage.
  5) Now, start the router and install by accepting all the default terms.
  6) In the last step, it asks for reboot, press reboot and while it is rebooting, remove the disk file by clicking on devices $- >$ optical drives and then remove disk.
  7) Again reboot and configure the interfaces provided by giving the subnet to the interfaces. You can assign static address or dynamically assign address using DHCP.

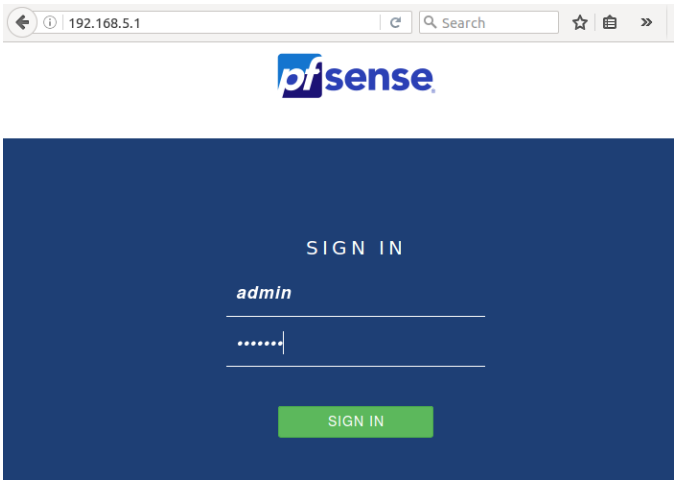

Fig. 3. Pfsense login-page

- **Configuration of the Router:** Initially, the router will block all the packets passing through it. Hence, we have to add rule to allow packets through the interface.
  1) Open the web interface of the router by entering the LAN interface ip address.
  2) The username is ”admin” and the password is ”pfsense” to login to the interface.
  3) Once entered, you can change the firewall rules by clicking on firewall option and then on rules. Now, you can configure your own rules depending on which packet you want to allow and which packet not to.

  Once configured, you can run create host machines, and dns servers etc on different interfaces and now will be able to perform some of the attacks on the host machines andd other servers.

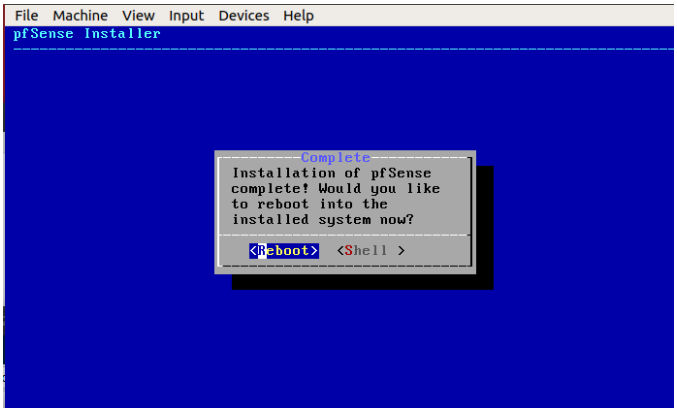

Fig. 4. configuring Pfsense

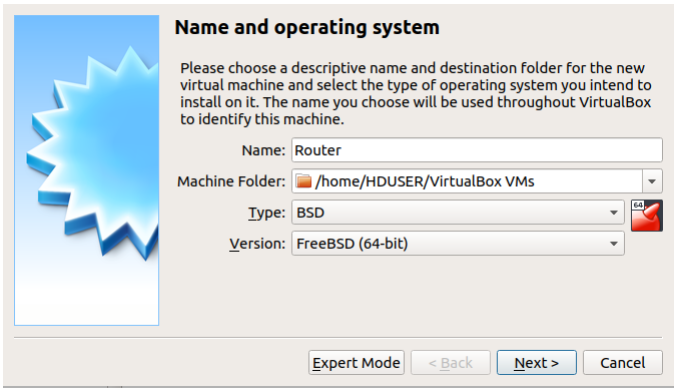

Fig. 5. configuring ISO with virtual-box

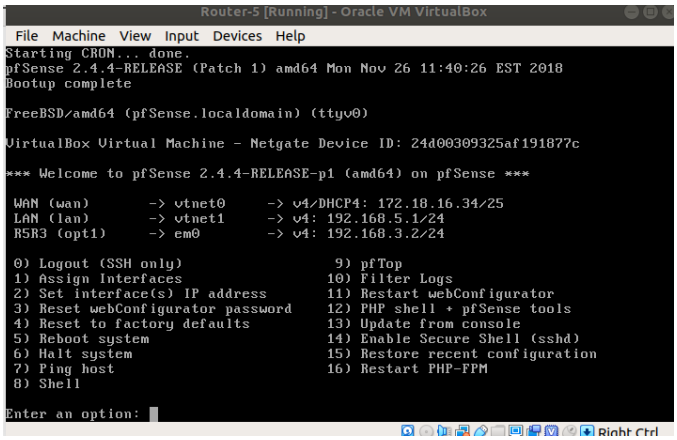

Fig. 6. configuraing router via terminal

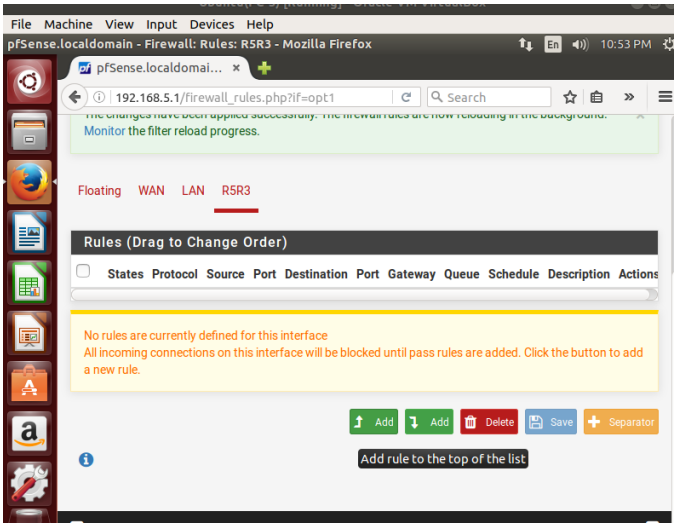

Fig. 7. Pfsense Web-Interface

IV. SECURITY ATTACKS

We have actually preformed basic security attacks using tools pre-installed in kali linux. which are give as follow:

1) **Analyzing the network traffics:**
   It reviews methods and techniques for packet analysis. Using $Wireshark$ can perform this packet and network analysis.
2) **Detecting live systems and understanding result:**
   - *Port scanning:*port scanning is a process to probe a server or host for open orts and used to verify security policies of their networks and by attackers to identify network services running on a host and exploit vulnerabilities.
     we have used $nmap$ utility of kali to perform this all.
   - *OS fingerprinting:* It is the process of determining the operating system used by a host on a network and configuration that is uses. also for this we have used $nmap$ utility with different option.

V. FUTURE WORK

we also want to perform other these other types of attack in the future:

- DNS spoofing
- DNS cache poisoning
- DGA detection