

California State University, San Bernardino CSUSB ScholarWorks

Electronic Theses, Projects, and Dissertations

Office of Graduate Studies

6-2019

BUILDING A SECURE NETWORK TEST ENVIRONMENT USING VIRTUAL MACHINES

Byungjin Lee

Follow this and additional works at: https://scholarworks.lib.csusb.edu/etd

Part of the Computer Engineering Commons

Recommended Citation

Lee, Byungjin, "BUILDING A SECURE NETWORK TEST ENVIRONMENT USING VIRTUAL MACHINES" (2019). *Electronic Theses, Projects, and Dissertations*. 947. https://scholarworks.lib.csusb.edu/etd/947

This Project is brought to you for free and open access by the Office of Graduate Studies at CSUSB ScholarWorks. It has been accepted for inclusion in Electronic Theses, Projects, and Dissertations by an authorized administrator of CSUSB ScholarWorks. For more information, please contact scholarworks@csusb.edu.

Building a secure network test environment using virtual machines

A Project

Presented to the

Faculty of

JHB College of Business and Public Administration,

California State University

San Bernardino

In Partial Fulfilment

of the Requirements for the Degree

Master of Information Systems and Technology

by

Byungjin Lee

June 2019

Building a secure network test environment using virtual machines

A Project

Presented to the

Faculty of

JHB College of Business and Public Administration,

California State University

San Bernardino

by

Byungjin Lee

June 2019

Approved by:

Joon Son, PhD., Advisor

Date

Conrad Shayo, PhD, Reader

Jay Varzandeh, PhD., Chair, Information & Decision Sciences Department

Dedication

This project is wholeheartedly dedicated to my beloved parents, Minyeong Lee and Heejeong Min. They have been my source of inspiration and strength when I was riddled with the thoughts of giving up. My parents continually provide their moral, spiritual, emotional, and financial support. In addition, my beloved brother Byunggo Lee, sister in law Yuji Hyun, and niece Nawon Lee have been encouraging during my studies. To Annie, whose words of advice and encouragement led me to finish this project. Special thanks to Professor Conrad Shayo, for your instruction and support throughout the project. Lastly, I dedicated this project to Professor Joon Son, thank you for the guidance, strength, power of the mind, protection, and skills and for giving me a healthy life. All of these, I offer to you. Now I stand at another starting point. I will not forget the support and encouragement of many people and must do my best in my life.

Abstract

The objective of this project is to provide an overview of how to create a secure network test environment using virtual machines with Red Hat CentOS 7. Using virtual machines to create a secure network test environment simplify the workflow of testing several servers including network segmentation, network path redundancy, and traffic control using a firewall. This study suggests a set of guidelines for building a secure network test environment that includes a Domain Name Server (DNS), Web Server, File Transfer Protocol (FTP) Server, and a firewall. The documentation provided in this project is primarily useful for IT students looking to recreate a similar environment of their own and to practice special skills needed within their field of study.

Keywords: Secure network test environment, Virtual machine, Red Hat CentOS 7, Windows, DNS, Web Server, FTP, Firewall, Iptables

Dedication	i
Abstract	ii
1. Introduction	1
2. Problem Statement	2
3. Project Materials	2
4. Project Structure	4
5. Literature Review	4
6. Project Methodology	5
7. DNS, Web server, and FTP Components, Implementation, and Analysis	6
7.1. Test case for Domain Name Server (DNS)	6
7.1.1 Domain Name Server (DNS) – Components	7
7.1.2 Domain Name Server (DNS) – Implementation and Analysis	
7.2. Test case for Web Server	9
7.2.1 Web Server – Components	9
7.2.2 Web Server – Implementation and Analysis	
7.3. Test case for File Transfer Protocol (FTP) Server	
7.3.1 File Transfer Protocol (FTP) – Components	
7.3.2 File Transfer Protocol (FTP) – Implementation and Analysis	
8. Firewall Components and Analysis	
8.1. Test case for Firewall	
8.1.1 Access control policy specifications	
8.1.2 Firewall - Components	14
8.1.3 Firewall - Analysis	
9. Penetration Test	
9.1 Vulnerability testing done by Cyber Graduate Students	
9.2 SYN flood	
9.2.1 SYN flood attacks – Test	
9.2.2 SYN flood attacks – Solution	

9.3 SYN-ACK	
9.3.1 SYN-ACK attacks – Test	
9.3.2 SYN-ACK attacks – Solution	
Conclusion	
References	24
Appendix	
1. Domain Name Server (DNS) – Configurations	
2. Web Server – Configurations	
3. File Transfer Protocol (FTP) Server– Configurations	
4. Firewall – Configurations	41

1. Introduction

With the rapid development of electronic devices and the Internet of Things, there are numerous network security threats in our daily lives. For decades, network security exploits happen frequently. These threats include malicious programs, worm, Trojan horse, spyware, rootkit, and ransomware. For this reason, most organizations require secured servers within their network to protect their data.

Students are met with several major challenges when it comes to building servers, one being budget constraints. Nevertheless, virtual machines make it possible to create a diversified virtual network lab at a minimal fee. Tsihouridis et al. (2014) noted that "students were able to use both real and virtual lab according to their educational needs." "A virtual machine (VM) is a logical process (most often an operating system) that interfaces with emulated hardware and is managed by an underlying control program. Originally, virtual machines were run on mainframes to provide resource multiplexing and isolation" (Gum, 1983). "Most modern virtual machine systems use the virtual machine monitor (VMM) model for managing and controlling individual virtual machines" (Zhao, Borders & Prakash, 2009).

Although Windows is a very popular system, this virtual environment also focuses on Linux systems. Linux is a completely open-source operating system that is more secure in comparison to other operating systems, even Windows. "The Linux OS has had about 60 to 100 viruses listed until date. But now-a-days unfortunately none of these are actively working. On the other hand, there are more than 60K kwon viruses in Windows." (Abhilash & Abhinay, 2015). For example, Linux does not require the installation of an anti-virus program because the virus cannot execute without the administrator's password. This system also offers Iptables, an application that allows a system administrator to configure the specific access control rules provided by the Linux kernel's Netfilter framework. The objective of this project is to build a secure network test environment utilizing virtual machines consisting of the Linux system as well as Windows system for IT students looking to expand their skills at minimal costs.

2. Problem Statement

The objective of this project is to provide IT students with suggested guidelines for building their own secure network test environments using virtual machines. The documentation includes how many machines are required, how the servers should be configured, which open-source tools are needed and how to ensure the secure network works. This allows student users to practice their desired network security skills at the minimal costs of \$918 compared to using physical machines that may cost well over \$8,000 depending on the types and number of servers used. Detailed costs can be reviewed in the Project Materials section below.

3. Project Materials

The design of this project requires one physical computer that has multiple virtual machines running on it. The hardware specifications are as follows:

< Physical Machine > - \$ 768.00

- CPU Intel ® Core TM i7-7500U @ 2.70GHz 2.90
- RAM 12 GB
- Operating System Windows 10 64-bit
- Hardware Solid State Drive 1TB

<VMware Workstation Pro 15> - \$150.00

• Memory - 2 GM

- Processors 1
- Hard Disk (SCSI) –80 GB
- CD/DVD (IDE) CentOS 7 and Auto Detect
- Network Adapter NAT and Bridged

As previously mentioned, it is more cost effective to build a secure network environment using virtual machines. The total cost for building the physical test environment using the physical machines shown below is \$ 9,291.00. Here is an example price comparison of how much building a similar environment using physical machines would be.

< Server > requires 2 machines

• PowerEdge R640 Rack Server - \$1,969.00

< Firewall > requires 1 machine

• Cisco Meraki MX100 Cloud Managed Security Appliance - \$3,447.00

< Switch > requires 2 machines

• Netgear JGS524 ProSafe 24 Port Gigabit Ethernet Desktop Switch - \$185.00

< Physical computer > requires 2 machines

 HP Pavilion 15.6-inch FHD 1080P Laptop PC, Intel Core i7 Processor, 12GB Memory, 1TB Hard Drive, Backlit Keyboard, Webcam, Bluetooth, USB 3.1, Windows 10 - \$768.00

The thus, building a test environment using virtual machines is significantly more costeffective than a test environment using physical machines. There are selected the price based on Amazon website.

4. Project Structure

The structure of this project is for building a secure network test environment using virtual machines, as shown in Figure 1.



Figure 1. The flow of the entire project.

5. Literature Review

This project presents the experiences from using virtual machines to test a secure network environment on Linux or Windows operating systems. "Virtual Machine technology has increased in popularity over the last few years because production environments have had success using Virtual Machines to reduce many types of operational costs" (Baker Hart, 2002). In addition, "with limited educational resources and dramatically increasing number of students, efficient and timely access to physical computer labs becomes more difficult [for students]" (Alharbi, 2018). Therefore, it is possible for a virtual machine to support self-contained and potable security experiences to improve student technical skills because it is essentially another computer inside a physical computer. "The resources of lab computer systems can be utilized more effectively, multiple environments can be configured quickly and easily, and access to external resources can be provided without permitting attacks to those resources" (Bulbrook, 2006).

A virtual machine requires an operating system such as Linux or Window and several programs may operate separately on the same physical computer. Although one may think guidelines for building a secure network test environment are readily available, it has proven to be difficult to come across one. As a result, building a secure network test environment using virtual machines and the Linux operating system, as presented in this project, provides a unique, cost-effective and easy guide for IT students to improve their technical skills.

6. Project Methodology

A configuration of network servers run based on access control policy specification implemented using virtual machines. To accomplish the final network architecture, the 3 test environments such as Domain Name Server (DNS), Web Server, and File Transfer Protocol (FTP) Server should be prerequisites to execute a secure network test environment. The goal of this architecture is to implement a test environment through several virtual machines within the private network and one virtual machine with the public network. For example, Server A has a private network of 10.0.0.0/24 with bridged and a public network of 192.168.111.0/24 with Network

Address Translate (NAT). Server B and Linux client have a private network of 10.0.0.0/24. On the other hand, Window client has a public network of 192.168.111.0/24.

7. DNS, Web server, and FTP Components and Analysis

The final network architecture shown in Figure 2, building the 3 virtual environments such as Domain Name Server (DNS), Web Server, and File Transfer Protocol (FTP) Server is necessary for a secure network test environment, which I will build in a later chapter.



Figure 2. Secure network test environment using virtual machines

7.1 Test case for Domain Name Server (DNS)

Domain Name Server (DNS) serves a specific purpose in this project and is necessary for a secure network test environment. A DNS is a computer server that contains a database of public IP addresses and associated hostnames. Mainly, a DNS is used to resolve or translate the requested IP addresses (Margaret, 2019). In order to build the DNS server, two things are required: a Caching-only name Server and a Master Server. A Caching-only name Server, in a secured environment with a strict firewall implementation, allows local clients to obtain name service without having to pierce the firewall. A Master Server is authoritative and contains a complete copy of all information for all hosts in the DNS domain. Lastly, a Web server processes incoming network requests over HTTP (Port 80).

7.1.1 Domain Name Server (DNS) – Components

As shown in Figure 3, Server A (10.1.1.1) has the Caching-only Name Server and Master Server. Server B (10.1.1.20) has the Web Server. Both server A (10.1.1.1) and server B (10.1.1.20) support for a highly configurable secure network environment. Detailed configurations can be reviewed in the Appendix (Domain Name Server (DNS) – Configurations).

• Server A – Caching-only Name Server and Master Server



• Server B – Web Server

Figure 3. Domain Name Server (DNS)

7.1.2 Domain Name Server (DNS) – Implementation and Analysis

In order to implement the Domain Name Server (DNS), the Linux client requests not only the IP address to a Caching-only name Server which translates from A Uniform Resource Locator (URL) to IP address but also a Master Server which manages all information for hosts in the DNS domain then the Linux client can access the Web Server.

I tested and reviewed the proposed configuration and components to ensure they work as expected. As a result, I was able to verify the Domain Name Server (DNS) through Linux Client (10.1.1.10) as shown in Figure 4. Both Server A (10.1.1.1) and Server B (10.1.1.20) were successful through the Linux client (10.1.1.10). Here are the steps to verify if the system is correctly configured:

Step 1. A user in the Linux client (10.1.1.10) types <u>www.CSUSB.com</u>

Step 2. DNS into Server A (10.1.1.1) responds to Linux client (10.1.1.10)

Step 3. Linux client with IP (10.1.1.10) accesses Web Server into Server B (10.1.1.20)

Here is the analysis of Linux Client as shown in Figure 4



Figure 4. Linux Client can access the Sever B

7.2 Test case for Web Server

Web Servers serve a specific purpose in this project and is necessary for a secure network test environment. A Web Server is a computer server that stores and transmits data via the Internet (Art, 2010). They are mainly used to ultimately dictate the data upon the request of guest's browser. In order to build Web server, there are two things required. The first is a set of software subsystems or components needed to create a complete web hard (Pydio). The software needed include Linux, Apache, PHP, and MariaDB (LAPM). The second is a Web hard (Pydio). A web hard is an open-source file sharing for the practice of providing access to an online storage service and synchronization software that runs on the own server. (Kanghyun & Jongmoon. 2013).

7.2.1 Web Server – Components

The main goal of setting up this environment is for IT students to gain experience building a secure web server. More specifically, these students will learn how to configure a web hard. As shown in Figure 5, Server B (10.1.1.20) has the Linux, Apache, PHP, and MariaDB (LAPM), as well as the Web hard. Server B (10.1.1.20) supports for a highly configurable environment. Detailed configurations can be reviewed in the Appendix (Web Server – Configurations).



• Server B –Linux, Apache, PHP, and MariaDB (LAPM), and Web hard

Figure 5. Web Server

7.2.2 Web Server – Implementation and Analysis

In order to implement the Web Server, the Linux client requests the IP address to a Domain Name Server (DNS) then the Linux client can access a Web hard (Pydio) to share an open source file to an online storage service and synchronization software.

I tested and reviewed the proposed configurations and components to ensure they work as expected. As a result, I was able to verify if the Web server correctly functions through the Linux client. Here are the steps to verify if the system is correctly configured:

Step 1. A user in the Linux client (10.1.1.10) types 10.1.1.20/webhard/

Step 2. DNS into Server A (10.1.1.1) responds to Linux client (10.1.1.10)

Step 3. Log into Pydio (10.1.1.20) through identification (CSUSB) and password (1234)

Step 4. Admin access - admin in admin identification (admin) password (12345678)

Global options - English in default language Configurations storage – user identification (xeUser) and password (1234)

Add some users – identification CSUSB, email (<u>admin@csusb.com</u>), and password

(1234)

Step 5. Linux client (10.1.1.1) accesses Pydio (10.1.1.20)

Here is the analysis of Linux Client as shown in Figure 6



Figure 6. Linux Client can access the Sever B

7.3 Test case for File Transfer Protocol (FTP) Server

File Transfer Protocol (FTP) Server serves a specific purpose in this project and is necessary for a secure network test environment. An FTP Server is a computer server that communicates between the client and the server to control data transmission. Mainly, FTP uses credentials in the form of username and password in order to allow or deny authorization. In order to secure an FTP server, Very Secure FTPD (VSFTPD) is necessary because it is designed to secure systems against most common attacks, providing for more security, scalability and simplicity (Chris, n.d.).

7.3.1 File Transfer Protocol (FTP) – Components

As shown in Figure 7, Server B (10.1.1.20) has Very Secure FTPD (VSFTPD). Server B (10.1.1.20) supports for a highly configurable security environment. Detailed configurations can be reviewed in the Appendix (File Transfer Protocol (FTP) – Configurations).



• Server B – Very Secure FTPD (VSFTPD) for server

Figure 7. File Transfer Protocol (FTP)

7.3.2 File Transfer Protocol (FTP) - Implementation and Analysis

In order to implement the File Transfer Protocol (FTP), the Linux client requests the IP address to a Domain Name Server (DNS) then the Linux client can access the File Transfer Protocol (FTP) to control data transmission to allow or deny authorization.

I tested and reviewed the proposed configuration and components to ensure they work as expected. As a result, I was able to verify the File Transfer Protocol (FTP) through Linux Client as shown in Figure 8. Server B was successful through Linux Client. Here are the steps to verify if the system is correctly configured:

Step 1. A user in the Linux client (10.1.1.10) machine types ncftp 10.1.1.20

Step 2. DNS into Server A (10.1.1.1) responds to Linux client (10.1.1.10)

Step 3. Logging in File Transfer Protocol (FTP) server (10.1.1.20)

Step 4. Linux client (10.1.1.10) accesses successfully

Here is the analysis of Linux Client as shown in Figure 8

```
root@localhost:~ _ ■ ×
File Edit View Search Terminal Help
[root@localhost ~]# ncftp 10.1.1.20
NcFTP 3.2.5 (Feb 02, 2011) by Mike Gleason (http://www.NcFTP.com/contact/).
Connecting to 10.1.1.20...
(vsFTPd 3.0.2)
Logging in...
Login successful.
Logged in to 10.1.1.20.
ncftp / > ■
```

8. Firewall Components, Implementation, and Analysis

Now, students are ready to build a secure network test environment and should successfully reach these objectives:

- 1. Translate security policy specification to actual implementation via Iptables.
- 2. Test if the firewall correctly enforces the security policy specifications and explore the vulnerabilities of the firewall.

8.1 Test case for Firewall

Firewalls serve a specific purpose in this project and is necessary for a secure network test environment. A Firewall is as security setting that is intended to act as a barrier or shield from unauthorized internet users from accessing a private network. Mainly, a Firewall is used to monitor the packets of data between servers and clients to accept or reject request based on access control policy specification such as Iptables. Iptables is a generic table structure for access control specification rules as part of the netfilter framework that facilitates Network Address Translation (NAT), packet filtering, and packet mangling in the Linux operating systems. (Margaret, 2005)

8.1.1 Access control policy specifications

I configured three Iptables in the Firewall which can enforce the access control specification. If I do not configure correctly both letters and spaces as well, Iptables will not operate. Detailed configurations can be reviewed in the Appendix (Firewall – Configurations). Here is a list of access control rules to enforce:

Rule 1. The users (any machine) within a private network can access the public network.

Rule 2. If the Window Client within a public network attempts to access the Web Server or the FTP Server, which is installed on Server B, the Firewall, that is installed on Server A, allows access into Server B within the private network.

Rule 3. The users (any machine) within a public network cannot access the private network other than the exception shared in Rule 2.

8.1.2 Firewall - Components

As shown in Figure 9, Server A has two IP addresses: one for private network address of 10.1.1.0/24 and another one for public network address of 192.168.111.0/24. It also contains the Iptables. Server B (10.1.1.20) runs the Web Server and FTP Server, which was installed in the previous chapter. Both Server A and Server B provide for a highly configurable security environment as shown in Figure 9. Detailed configurations can be reviewed in the Appendix (Firewall – Configurations).

- Server A Two IP addresses: one for private network address of 10.1.1.0/24 and another one for public network address of 192.168.111.0/24, and iptables
- Server B Web Server (Port 80) and FTP Server (Port 21) run two services



• Window Client – Nmap

Figure 9. Firewall

8.1.3 Firewall – Analysis

I tested and reviewed the proposed configuration and components to ensure they work as expected. The following three subsections will explain how I tested and verified if the firewall (Iptables) is able to correctly enforce the access control rules. Here is the test result of Rule 1 for access control specifications as shown in Figure 10:

	CAS - California State University, San Bernardino - Mozilla Firefox			×
🙈 CAS – California State Uni 🗙	+			
< → ♂ @	🛈 🚔 https://weblogon.csusb.edu/cas/login?service=https%3A%2F%2Fidp.csusb.edu%2Fidp 🗧 🚥 😴 🏠	IIIN	Ð	=
myCoyote	Directory Map & Directions Support CSUSB		٩	
	Admissions Academics Library Athletics Campus Life About Us			
	Login Technology Support Center			
	Please sign-in to access your account			
	Pasword			

Figure 10. Linux client with private network address accesses the public network address

Here is the test result of Rule 2 for access control specifications as shown in Figure 11 and Figure 12, Figure 13, and Figure 14:

```
< Web Server >
```

Step 1. A user in the window client (DHCP) types 10.1.1.20

Step 2. Firewall in Server A checks Iptables then responds to window client (DHCP)

Step 3. Window client (DHCP) tries to access Web Server (10.1.1.20)

Step 4. Window client (DHCP) can access successfully



Figure 11. Window client with public network address accesses the Web server with private

network address

•	Zenmap — 🗖 🗙
Sc <u>a</u> n <u>T</u> ools <u>P</u> rofile	<u>H</u> elp
Target: 192.168.111.1	00 V Profile: Scan Cancel
Command: nmap -sT	-p 80 -v -v 192.168.111.100
Hosts Services	Nmap Output Ports / Hosts Topology Host Details Scans
OS • Host	nmap -sT -p 80 -v -v 192.168.111.100
₩ 192.168.111.10	<pre>Starting Nmap 7.70 (https://nmap.org) at 2019-06-10 15:12 Pacific Daylight Time Initiating ARP Ping Scan at 15:12 Scanning 192.168.111.100 [1 port] Completed ARP Ping Scan at 15:12, 0.56s elapsed (1 total hosts) Initiating Parallel DNS resolution of 1 host. at 15:12, 0.00s elapsed Initiating Connect Scan at 15:12 Scanning 192.168.111.100 [1 port] Discovered open port 80/tcp on 192.168.111.100 Completed Connect Scan at 15:12, 0.00s elapsed (1 total ports) Nmap scan report for 192.168.111.100 Host is up, received arp-response (0.012s latency). Scanned at 2019-06-10 15:12:12 Pacific Daylight Time for 2s PORT STATE SERVICE REASON 80/tcp open http syn-ack MAC Address: 00:0C:29:BB:78:11 (VMware) Read data files from: C:\Program Files (x86)\Nmap Nmap done: 1 IP address (1 host up) scanned in 3.42 seconds Raw packets sent: 1 (28B) Rcvd: 1 (28B)</pre>
Filter Hests	
Filter Hosts	

Figure 12. Nmap was used to scan HTTP (Port 80) state

< File Transfer Protocol (FTP) >

Step 1. A user in the window client (DHCP) types host (10.1.1.20), username (anonymous), and password (1234)

Step 2. Firewall in Server A checks Iptables then responds to window client (DHCP)

Step 3. Window client (DHCP) tries to access File Transfer Protocol (FTP) server (10.1.1.20)

Step 4. Window client (DHCP) can access successfully

File Edit View Transfer Server Bookmarks Help New version available!				
Host: 10.1.1.20 Username: anonymous Password: ••••	Port: Quickconnect -			
Response: 150 Accepted data connection Response: 226-Options: -a -I Response: 226 5 matches total Status: Directory listing successful	^ ~			
Local site: \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \	Remote site: /pub/file1 v pub/file1 file1			
Filename Filesize Filetype Last modified	Filename Filesize Filetype Last mod			
E C: Local Disk D: CD Drive	vmlinuz-3.10.0-123.el7.x86_64 4,902.656 X86_64 F 5/21/201 vmlinuz-3.10.0-957.12.2.el7.x86_64 6,643,904 X86_64 F 5/21/201 vmlinuz-3.10.0-957.el7.x86_64 6,639,904 X86_64 F 5/21/201			
2 directories	3 files. Total size: 18,186,464 bytes			
Server/Local file Direc Remote file Size Priority Status Queued files Failed transfers Successful transfers				
	🕅 🕎 Queue: empty 🔍 🔹 📑			

Figure 13. Window client with public network address accesses the File Transfer Protocol (FTP)

Zenmap Sc<u>a</u>n <u>T</u>ools <u>P</u>rofile <u>H</u>elp Profile: ✓ Scan Cancel Target: 192.168.111.100 Command: nmap -sT -p 21 -v -v 192.168.111.100 Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans OS • Host 192.168.111.10 ✓ Details nmap -sT -p 21 -v -v 192.168.111.100 PORT STATE SERVICE REASON 21/tcp open ftp syn-ack MA<u>C Address:</u> 00:00:29:88:78:11 (VMware) Read data files from: C:\Program Files (x86)\Nmap Nmap done: 1 IP address (1 host up) scanned in 4.70 seconds Raw packets sent: 1 (28B) | Rcvd: 1 (28B) Filter Hosts

server with private network address

Figure 14. Nmap was used to scan FTP (Port 21) state

9. Penetration Test

I wanted to see if my security test environment can be efficiently used for educating IT students. In order to do so, I had two Cyber Security Graduate Students from California State University, San Bernardino conduct penetration tests on my secure network test environment to see if they could find any vulnerabilities.

9.1 Vulnerability testing done by Cyber Graduate Students

I first asked them to recreate the steps and commands I previously used on Nmap, as shown in the Firewall-Analysis section of this project. Then, both of them used other Nmap commands of their choice to further try and scan for vulnerabilities of the firewall. This process is needed to see if the firewall is at least faithfully following the access control rules and so that the Graduate Students get familiarized with the secure network test environment, as shown in Figure 15, and





Figure 15. Penetration test- Nmap

Building a secure network test environment using virtual machines



Figure 16. Scan for vulnerabilities of the firewall

9.2 SYN flood

I gave them Iptables rules and had them scan for vulnerabilities of the firewall again. They were able to find two vulnerabilities of Iptables. One of them is that the Firewall cannot protect against SYN flood attacks.

9.2.1 SYN flood attacks – Test

The Graduate Students used Hping3 and Wireshark security tools to analyze its vulnerability of Iptables. Finally, they tested SYN flood attacks from the Linux Client with a public IP address to the Web Server with a private IP address. They then verified the Firewall does not fully protect HTTP from SYN flood attacks (200,471 packets transmitted, 186,438 packets received, 7% packet loss) as shown in Figure 17.

	root@localhost:-	· · · · · · · · · · · · · · · · · · ·	_ = ×	
File Edit View Search Termin	al Help			
len=46 ip=10.1.1.20ttl=64 D	<pre>>F id=0 sport=80 flags=SA se >F id=0 sport=80 flags=SA se</pre>	eq=20452 win=29200 rtt=0.7 ms		
len=46 ip=10.1.1.20ttl=64 D	OF id=0 sport=80 flags=SA se	eq=20454 win=29200 rtt=0.5 ms		×
len=46 ip=10.1.1.20ttl=64 D)F id=0 sport=80 flags=SA se	eq=20455 win=29200 rtt=0.5 ms		
len=46 ip=10.1.1.20ttl=64 D)F id=0 sport=80 flags=SA se	eq=20456 win=29200 rtt=0.4 ms		
len=46 1p=10.1.1.20ttL=64 D	<pre>>> id=0 sport=80 flags=5A se >> id=0 sport=80 flags=5A se</pre>	eq=20457 win=29200 rtt=0.3 ms		
len=46 in=10.1.1.20ttl=64 D	OF id=8 sport=80 flags=54 se	eq=20450 win=29200 ftt=0.5 ms		
len=46 ip=10.1.1.20 ttl=64 D	OF id=0 sport=80 flags=SA se	eq=20460 win=29200 rtt=0.5 ms		
len=46 ip=10.1.1.20ttl=64 D	OF id=0 sport=80 flags=SA se	eq=20461 win=29200 rtt=0.4 ms		
len=46 ip=10.1.1.20 ttl=64 D	DF id=0 sport=80 flags=SA se	eq=20462 win=29200 rtt=0.6 ms		the second se
^c				
10.1.1.20 nping statistic	196429 packets received	The section for the section of the s		
round-trip min/avg/max = 0	2/2 9/1827 8 ms	7% packet Loss		the second se
[root@localhost -]#				
	conformation and a second second second second	Frankrise and when we found a summaries		_ 0 ×
File Edit View Go Capture	Analyze Statistics Telephony Too	ols Internals Help		
			•	
r mater.		ressource coon oppiny save		
No. Time Source	Destination	Protoci Lengt Info		
23788 7.276602755 192.168.1	11.200 10.1.1.20	TCP 54 11626 > http	[SYN] Seq=0 Win=512 L	en=0
23789 7.276663315 10.1.1.20	192.168.111.200	TCP 60 http > 11624	[SYN, ACK] Seq=0 Ack=	1 Win=29200 Len=0 MSS=1460
23790 7.276683772 192.168.1	11.200 10.1.1.20	TCP 54 11624 > http	[RST] Seq=1 Win=0 Len	=0
23/91 /.2/6/24950 10.1.1.20	192.168.111.200	TCP 60 http > 11625	[SYN, ACK] Seq=0 ACK=	1 W1n=29200 Len=0 M55=1460
23792 7.276739340 192.108.1	11.200 10.1.1.20	TCP 54 11623 > http	[KS1] Seq=1 Win=0 Len	
23794 7 276838684 192 168 1	11.200 10.1.1.20	TCP 54 11628 > http	[STN] Segred Win=512 L	en=0
23795 7 277568419 10 1 1 20	197 168 111 200	TCP 60 http > 11626	SYN ACKI Seg-0 Ack-	1 Win-29200 Len-0 MSS-1460
	192.100.111.200	107 00 metp > 11020	ISIN, ACRI SCO-O ACR-	1 111-25200 201-0 155-1400
0000 00 50 55 00 53 57 00 00	20.25 fb +0.00 00 45 00 0	u cu let e		
0000 00 50 50 68 53 57 00 00	29 33 00 co 06 00 45 00 .P	v.sw jske.		
0020 6f 02 00 89 00 89 00 4c	48 1d b0 99 40 00 00 01 o.	L H@		
0030 00 00 00 00 00 01 20 46	48 45 4a 45 4f 45 44 45	F HEJEOEDE		
O ≝ eno16777736: <live capture="" in<="" p=""></live>	progr Packets: 111421 - Displayed	d: 111421 (100.0%)		Profile: Default

Figure 17. SYN flood attacks to the Firewall were successful

9.2.2 SYN flood attacks – Solution

They made new Iptables to protect against SYN flood attacks. The Graduate Students conducted another test using these new Iptables to verify if it works. As a result, the firewall now protected HTTP against SYN flood attacks (30,926 packets transmitted, 3624 packets received, 88% packet loss) as shown in Figure 18.

• iptables -I INPUT -p tcp --dport 80 -i eth0 -m state --state NEW -m recent --update -seconds 1 --hitcount 10 -j DROP

File Edit View Search Terminal Help Len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flag=5A seq=20452 win=29200 rtt=2.8 ms Len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flag=5A seq=20453 win=29200 rtt=2.7 ms Len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flag=5A seq=20455 win=29200 rtt=1.6 ms Len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flag=5A seq=20455 win=29200 rtt=1.6 ms Len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flag=5A seq=20455 win=29200 rtt=1.6 ms
len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flag=5A seq=20452 win=29200 rtt=2.8 ms len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flag=5A seq=20453 win=29200 rtt=2.7 ms len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flag=5A seq=20454 win=29200 rtt=1.7 ms len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flag=5A seq=20455 win=29200 rtt=1.6 ms
len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flags=SA seq=20454 win=29200 rtt=1.7 ms len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flags=SA seq=20455 win=29200 rtt=1.6 ms len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flags=SA seq=20456 win=29200 rtt=1.6 ms
lem=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flags=5A seq=20455 win=29200 rtt=1.6 ms
len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flags=5A seq=20456 win=29200 rtt=1.6 ms
]
ten=46 1p=10.1.1.20ttt=64 DF 1d=0 sport=80 ftags=SA sed=20457 win=29200 ftt-1.5 ms
Len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flags=5A seq=20458 win=29200 rtt=1.4 ms
Len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flag=5A seq=20459 win=29200 rtt=1.0 ms
len=46 ip=10.1.1.20ttl=64 DF id=0 sport=80 flag=5A seq=20461 win=29200 rtt=0.7 ms
len=46 ip=10.1.1.20 ttl=64 DF id=0 sport=80 flags=SA seg=20462 win=29200 rtt=0.7 ms
^c ·
10.1.1.20 hping statistic
30926 packets transmitted, 3624 packets received, 88% packet loss
Found-trip min/avg/max = 0.2/6.7/1033.4 ms
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
👁 👁 🛋 📕 🔬 🖹 🖀 🗙 C Q 🔄 🔶 🎸 🖄 🖾 🗐 🖬 I o 🗆 🖻 🔛 🕷 🖼 🗃
Filter: Expression Clear Apply Save
No. Time Source Destination Protoc Lengt Info
19498 61.50667571!192.168.111.200 10.1.1.20 TCP 54 11827 > http [RST] Seq=1 Win=0 Len=0
19499 61.506741361192.168.111.200 10.1.1.20 TCP 54 11829 > http [SYN] Seq=0 Win=512 Len=0
19500 61.5068123410.1.1.20 192.168.111.200 TCP 60 http > 11828 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
19501 01.500082441192.108.111.200 10.11.200 10.11.20 10P 54 11828 > http://stij.seg=1.Win=0.Len=0
19502 01.500007501122.100.111.200 10.1120 10. 54 14050 10.000 000 000 000 000 000 000 000 000
1950 61.500909131011120 192.100.111.200 10 10 10 10 10 10 10 10 10 10 10 10 1
19585 61.50707379!10.1.1.20 192.168.111.200 TCP 60 http > 11830 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
19506 61.50709310+192.168.111.200 10.1.1.20 TCP 54 11830 > http [RST] Seq=1 Win=0 Len=0
0000 ff ff ff ff ff 0a 00 27 00 00 06 08 00 45 00
0010 00 2c 51 16 00 00 80 11 f1 01 c0 a8 38 01 ff ff0
0020 ff ff e9 9f 21 a3 00 18 39 26 42 4a 4e 50 01 01
19839 68 68 31 18 68 68 69 69 69 69 69 69 69 69 70 150 avect 48099 (100 0%) Profile: Default

Figure 18. SYN flood attacks failure – Blocked by the Firewall

9.3 SYN-ACK

They tested against SYN-ACK attacks from the Linux Client with a private IP address to the Firewall with a public IP address to determine if it is stateful or stateless.

9.3.1 SYN-ACK attacks - Test

The Graduate Students used Hping3 and Wireshark security tools to analyze its vulnerability of Iptables. Finally, they sent several SYN-ACK packets from a private IP address to a public IP address. All SYN-ACK attacks (sent 242,335 Tx packets, received 242,335 Rx packets) passed the Firewall without first sending SYN of a Three-way handshake to the Firewall with a public IP address, as shown Figure 19.

					root@localhos	t:~		-	×			
File Ec	lit View	Search Te	rminal Hel	р								
[root@localhost ~]# hping3 -i ul -S -A -p 80 192.168.111.100 HPING 192.168.111.100 (eno16777736 192.168.111.100): SA set, 40 headers + 0 data bytes ^C 192.168.111.100 hping statistic												
round-t [root@l File Ec	trip min localhos Mit View	/avg/max t ~]# Go Captur	= 0.0/0.0 e Analyze	/0.0 ms	ephony Tool	s Internals F	Help			<u> </u>	_	a ×
•			🖻 🛅 🗙	C Q	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	, ⊼ ⊻ [(1) **	X	180		
Filter:					- Expr	ression Clear	Apply Save					
No.	Time	Source	e	Destina	tion	Protoc(L	engt Info					
42512	29.8562	2204:10.1.1	.10	192.168	.111.100	TCP	54 55462 > http	[SYN, ACK]	Seq=0 Ack	=1 Win=512 Len=0		
42513	3 29.8562	5516:10.1.1	.10	192.168	.111.100	TCP	54 55463 > http	[SYN, ACK]	Seq=0 Ack	=1 Win=512 Len=0		
42514	29.85642	2034(10.1.1	1.10	192.168	.111.100	TCP	54 55464 > http	[SYN, ACK]	Seq=0 Ack	=1 Win=512 Len=0		
42515	5 29.8564	5246:10.1.1	1.10	192.168	.111.100	TCP	54 55465 > http	[SYN, ACK]	Seq=0 Ack	=1 Win=512 Len=0		
42516	5 29.8566	1208:10.1.1	1.10	192.168	.111.100	TCP	54 55466 > http	[SYN, ACK]	Seq=0 Ack	=1 Win=512 Len=0		
42517	29.8566	7597!10.1.1	1.10	192.168	.111.100	TCP	54 55467 > http	[SYN, ACK]	Seq=0 Acl	=1 Win=512 Len=0		
42518	3 29.8568	4141(10.1.1	1.10	192.168	.111.100	TCP	54 55468 > http	[SYN, ACK]	Seq=0 Acl	=1 Win=512 Len=0		
42519	29.8569	9651(10.1.1	1.10	192.168	.111.100	TCP	54 55469 > http	[SYN, ACK]	Seq=0 Acl	=1 Win=512 Len=0		
42526	29.8570	352410.1.1	1.10	192.168	.111.100	TCP	54 55470 > http	[SYN, ACK]	Seq=0 Ack	<pre>x=1 Win=512 Len=0</pre>		
42521	29.85/1.	2091:10.1.1		192.108	.111.100	TCP	54 55471 > http	ISTN. ACKI	Sed=0 ACF	=1 WIN=512 Len=0		_
					IP	v4 Endpoints: ei	no16777736					×
						IPv4 Endpoi	nts: 6					
Addre	SS	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes					
192.16	8.56.1	29	2 447	29	2 447	0)					0
255.25	5.255.255	24	1 440	0	0	24	ł					1 440
10.1.1.	10	242 335	13 086 090	242 335	13 086 090	0)					0
192.16	8.111.100	242 335	13 086 090	0	0	242 335	;				13 08	6 090
239.25	5.255.250	4	864	0	0	4	ł					864
224.0.0	251	. 1	143	0	ő	. 1						143
224.0.0		1	145	0	0	-	-					1 15

Figure 19. SYN-ACK attacks to the Firewall were successful

9.3.2 SYN-ACK attacks – Solution

They made new Iptables to protect against SYN-ACK flood attacks. The Graduate Students conducted another test using these new Iptables to verify if it also works. As a result, the firewall now blocked SYN-ACK flood attacks (sent 113,933 Tx packets, received 0 Rx packets) as shown Figure 20.

iptables -A OUTPUT -p tcp --tcp-flags SYN.ACK SYN,ACK -m state --sate NEW -j
 DROP



Figure 20. SYN-ACK attacks failure – Blocked by the Firewall

As a result, both Cyber Security Graduate Students were successful in penetrating the system. Although the proposed configurations enforce security, it is impossible to create a 100% vulnerability-free system. Nonetheless, security can always be improved upon, which was evident through the Graduate Students' penetration tests. This clearly shows that the test environment can be an effective tool for IT students to learn from. The Cyber Graduate Students were able to secure the Firewall by adding new Iptables rules to prevent SYN flood attacks and SYN-ACK attacks.

Conclusion

This set of guidelines to build a secure network test environment using virtual machines provide guidance for IT students. This study provides the workflow of testing several servers including network segmentation, network path redundancy, and traffic control. In order accomplish this, a Domain Name Server (DNS), Web Server, File Transfer Protocol (FTP) Server, Caching-only Name Server, Master Server, and Firewall were installed within virtual machines. Graduate Students were provided with a secure network test environment to verify all services, to test the access control rules, to find vulnerabilities of the Firewall, and to create solutions to protect the Firewall vulnerabilities they found. The suggested architecture provided within these guidelines are invaluable for IT students to help them recreate a similar environment of their own and to improve their technical skills.

References

- Abhilash, P., Abhinay sri vasthav. V. (2015). Comparison of Windows and Linux Operating Systems in Advanced Features. *Journal of Engineering Research and Applications, 2*, pp.81-83
- Alharbi, A. H. (2018). A Portable Virtual LAB for Informatics Education using Open Source software MILAB. INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, 9(2), 142-147.
- Art. (2010, August). What Are Web Servers and Why Are They Needed? Retrieved from https://webhostinggeeks.com/blog/what-are-web-servers-and-why-are-they-needed/
- Baker Hart (2002). Building a Security Lab with Virtual Machines. *Global Information Assurance Certification Paper. SANS Institute*
- Bulbrook, H. (2006). Using virtual machines to provide a secure teaching lab environment. *White paper. Durham Technical Community College, Durham.*
- Chris. (n.d.) Probably the most secure and fastest FTP server for UNIX-like systems. Retrieved from <u>https://security.appspot.com/vsftpd.html</u>
- Gum, P. H. (1983). System/370 extended architecture: facilities for virtual machines. *IBM Journal* of Research and Development, 27(6), 530-544.
- Kanghyun, C., Jongmoon, J. (2013, July). Webhards make illegal sharing of files too easy. Retrieved from <u>http://koreajoongangdaily.joins.com/news/article/article.aspx?</u> aid=2974881

Margaret, R. (2019, May). Domain name system (DNS). Retrieved from <u>https://searchnetworkin</u> g.techtarget.com/definition/domain-name-system

Margaret, R. (2005, September). Iptables. Retrieved from https://whatis.techtarget.com/definition/

iptables

- Tsihouridis, C., Vavougios, D., Ioannidis, G. S., Alexias, A., Argyropoulos, C., & Poulios, S. (2014, December). Using sensors and data-loggers in an integrated mobile school-lab setting to teach Light and Optics. In 2014 International Conference on Interactive Collaborative Learning (ICL) (pp. 439-445). IEEE.
- Zhao, X., Borders, K., & Prakash, A. (2009). Virtual machine security systems. Advances in Computer Science and Engineering, 1, 339-365.

Appendix

1. Domain Name Server (DNS) - Configurations

Each machine requires a different process in order to be built. Here are the necessary components for each server machine and client machine.

Configurations of Server A:

1) Caching-only name server

1.1) Start the Linux operating systems (Server A), by clicking Applications / Terminal.

1.2) Type yum -y install bind bind-chroot

1.3) Type vi /etc/named.conf

1.3.1) Type :set number

1.3.1) Change IP address from 127.0.0.1 to any - around 13 columns

1.3.2) Change IP address from ::1 to none - around 14 columns

1.3.3) Change IP address from localhost to any - around 21 columns

	root@localhost:~ _ □ ×
File	Edit View Search Terminal Help
	4 // Provided by Red Hat bind package to configure the ISC BIND named(8) D NS
	5 // server as a caching only nameserver (as a localhost DNS resolver only).
	<pre>6 // 7 // See /usr/share/doc/bind*/sample/ for example named configuration file</pre>
	<pre>5. 8 // 9 // See the BIND Administrator's Reference Manual (ARM) for details about</pre>
	the
	<pre>10 // configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html</pre>
	11
	12 options {
	13 Listen-on port 53 (any;);
	14 Listen-on-vo port 53 { none; };
	15 directory /var/named;
	17 statistics-file "/var/named/data/named_stats_tyt".
	18 menstatistics-file "/var/named/data/named mem stats tyt".
	19 recursing-file "/yar/named/data/named, recursing":
	20 secroots-file "/var/named/data/named.secroots":
	<pre>21 allow-query { any; }; 22</pre>

1.4) Change named for active

1.4.1) Type systemctl status named

1.4.2) Type systemctl restart named

1.4.3) Type systemctl enable named

root@localhost:~	-		×
File Edit View Search Terminal Help			
Active: active (running) since Wed 2019-07-17 16:30:00 PDT; 12min a Process: 7522 ExecStart=/usr/sbin/named -u named -c \${NAMEDCONF} \$0P e=exited, status=0/SUCCESS) Process: 7480 ExecStartPre=/bin/bash -c if [! "\$DISABLE_ZONE_CHECKI s"]; then /usr/sbin/named-checkconf -z "\$NAMEDCONF"; else echo "Check e files is disabled"; fi (code=exited, status=0/SUCCESS) Main PID: 7534 (named) Tasks: 4 CGroup: /system.slice/named.service -7534 /usr/sbin/named -u named -c /etc/named.conf	go TION NG" ing	IS (== of	cod "ye zon

1.5) Change firewall

1.5.1) Type firewall-config

1.5.2) Change configuration from runtime to permanent

1.5.3) Click dns in public zone

1.5.4)	Click	reload	firewal	lld	in	options
--------	-------	--------	---------	-----	----	---------

Firewall Configuration _ 🗖 🗸 🗸						
File Options View	ile Options View Help					
✓ Active Bindings	Configuration: Permanen	t 🕶				
Connections Palm Spring (ens 32) Default Zone: public San Bernardino (eno: Default Zone: public virbr0 (virbr0) Default Zone: public Interfaces Sources	Zones Services A firewalld zone defines th bound to the zone. The zone	IPSets IPSET I				
Change Zone	+ > - G	freeipa-ldap				
Connection to firewalld established.						

Default Zone: public Log Denied: off Panic Mode: disabled Automatic Helpers: system (on) Lockdown: disabled

2) Master name server

2.1) Start the Linux operating systems (Server A), by clicking Applications / Terminal.

2.2) Type vi /etc/named.conf

2.2.1) Type :set number

2.2.2) zone "CSUSB.com" IN { - around 62 columns

type master;

file "CSUSB.com.db";

allow-update { none; };

};"

```
root@localhost:~
                                                                                     ×
                                                                                 _
File Edit View Search Terminal Help
                 session-keyfile "/run/named/session.key";
     44
     45 };
    46
     47 logging {
     48
                 channel default_debug {
     49
                          file "data/named.run";
                          severity dynamic;
     50
     51
                 };
     52 };
     53
     54 zone "." IN {
                 type hint;
     55
                 file "named.ca";
     56
     57 };
     58
    59 include "/etc/named.rfc1912.zones";
60 include "/etc/named.root.key";
     61
     62 zone "CSUSB.com" IN {
               type master;
     63
                file "CSUSB.com.db";
     64
                allow-update { none; };
     65
     <mark>66</mark>};
set number:
```

2.2) Type cd /var/named

2.3) Type touch CSUSB.com.db

2.4) Type vi CSUSB.com.db

2.4.1) \$TTL	3H		
@	SOA	@	root. (2 1D 1H 1W 1H)
	IN	NS	@
	IN	А	10.1.1.1

www IN A 10.1.1.20

					root@localhost:/var/named _	×
File	Edit	View	Search	Terminal	Help	
\$TTL @			3H SOA IN IN	@ NS A	root. (2 1D 1H 1W 1H) @ 10.1.1.1	
www			IN	А	10.1.1.20	- 11
~						
~						
~						
~						
~						
~						
~						
~						
~						
_						
~						
~						
~						
~						
~						
~						
~						

2.5) Change named for active

2.5.1) Type systemctl status named

2.5.2) Type systemctl restart named

2.5.3) Type systemctl enable named

			root@	localhost:~	,			-		×
File Edit Viev	v Search Tern	inal Help								
Active: a Process: 7 e=exited, st Process: 7 s"]; then / e files is d Main PID: 7 Tasks: 4 CGroup: /	<pre>:tive (runnin 322 ExecStart atus=0/SUCCES 480 ExecStart usr/sbin/name isabled"; fi 534 (named) system.slice, -7534 /usr/sl</pre>	g) since =/usr/sbi S) Pre=/bin/ d-checkcc (code=exi named.ser in/named	Wed 2 in/nam /bash onf -z ited, rvice -u na	019-07-1 ed -u na -c if ["\$NAMED status=0 med -c /	7 16:30:0 med -c \${ ! "\$DISAE CONF"; el /SUCCESS)	00 PDT; [NAMEDCO BLE_ZONE se echo	12min ag NF} \$OP _CHECKII "Check:	go TION NG" ing	IS ((od 'ye zon

Configurations of Server B:

3) Web Server

3.1) Start the Linux operating systems (Server B), by clicking Applications / Terminal.

3.2) Type cd /var/www/html

3.3) Type touch index.html

3.4) Type vi index.html

3.4.1) California State University, San Bernardino

						root@localhost:~		—	×
File	Edit	View	Search	Terminal	Help				
≤h1> ~	Cali	forni	a State	Univer	sity,	SanBernardino.			
~									- 8
~									- 8
									- 8
									- 8
~									- 8
~									- 8
~									- 8
									- 8
									- 8
~									- 8
~									- 8
~									
									- 8
~									
									- 8
~									- 8
"/vai	-/~~~	/html	/index.	html" 1	_, 550	2			

3.5) Change firewall

3.5.1) Type firewall-config

3.5.2) Change configuration from runtime to permanent

3.5.3) Click http in public zone

3.5.4) Click reload firewalld in options

		Firewall Configuration _ 🗆 🗖 🗙
File Options View	Help	
✓ Active Bindings	Configuration: Permanent	-
Connections Palm Spring (ens32) Default Zone: public San Bernardino (eno: Default Zone: public virbr0 (virbr0) Default Zone: public	Zones Services II A firewalld zone defines the bound to the zone. The zone icmp filters and rich rules. The block	PSets level of trust for network connections, interfaces and source addresses e combines services, ports, protocols, masquerading, port/packet forwarding, e zone can be bound to interfaces and source addresses.
Default Zone: public Interfaces Sources	dmz drop external home internal public trusted work	Here you can define which services are trusted in the zone. Trusted services are accessible from all hosts and networks that can reach the machine from connections, interfaces and sources bound to this zone. Service ganglia-master git gre high-availability hittp hittps imap ipp ipp ipp
Connection to firewalld	established.	

Default Zone: public Log Denied: off Panic Mode: disabled Automatic Helpers: system (on) Lockdown: disabled

3.6) Change named for active

3.6.1) Type systemctl status named

3.6.2) Type systemctl restart named

<pre>File Edit View Search Terminal Help Active: active (running) since Wed 2019-07-17 16:30:00 PDT; 12min ago Process: 7522 ExecStart=/usr/sbin/named -u named -c \${NAMEDCONF} \$0PTIONS (cod e=exited, status=0/SUCCESS) Process: 7480 ExecStartPre=/bin/bash -c if [! "\$DISABLE_ZONE_CHECKING" == "ye s"]; then /usr/sbin/named-checkconf -z "\$NAMEDCONF"; else echo "Checking of zon e files is disabled"; fi (code=exited, status=0/SUCCESS) Main PID: 7534 (named)</pre>	root@localhost:~	-		×
<pre>Active: active (running) since Wed 2019-07-17 16:30:00 PDT; 12min ago Process: 7522 ExecStart=/usr/sbin/named -u named -c \${NAMEDCONF} \$OPTIONS (cod e=exited, status=0/SUCCESS) Process: 7480 ExecStartPre=/bin/bash -c if [! "\$DISABLE_ZONE_CHECKING" == "ye s"]; then /usr/sbin/named-checkconf -z "\$NAMEDCONF"; else echo "Checking of zon e files is disabled"; fi (code=exited, status=0/SUCCESS) Main PID: 7534 (named)</pre>	File Edit View Search Terminal Help			
Tasks: 4 CGroup: /system.slice/named.service	Active: active (running) since Wed 2019-07-17 16:30:00 PDT; 12min ag Process: 7522 ExecStart=/usr/sbin/named -u named -c \${NAMEDCONF} \$0PT e=exited, status=0/SUCCESS) Process: 7480 ExecStartPre=/bin/bash -c if [! "\$DISABLE_ZONE_CHECKIN s"]; then /usr/sbin/named-checkconf -z "\$NAMEDCONF"; else echo "Check: e files is disabled"; fi (code=exited, status=0/SUCCESS) Main PID: 7534 (named) Tasks: 4 CGroup: /system.slice/named.service	30 FION NG" ing	IS (== of	cod "ye zon

2. Web Server – Configurations

Each machine requires a different process in order to be built. Here are the necessary components for each server machine and client machine.

Configurations of Server B:

1) MariaDB

1.1) Start the Linux operating systems (Server B), by clicking Applications / Firefox web browser.

1.2) Type http://www.mariadb.org/

1.2.1) Click download mariadb now! then download 10.4.6

kind of support relationship with any	systema)					java source jar			
of the MariaDB support providers.	marladb-10.3.16-linux- glibc_214-i686.tar.gz (requires GLIBC_2.14+)	gzipped tar file	Linux x86	699.2 MB	Instructions				
	mariadb-10.3.16-linux- i686.tar.gz	gzipped tar file	Linux x86	573.5 MB	Checksum	CPU			
	Red Hat, Fedora, and CentOS Packages	RPM Package	RedHat/CentOS /Fedora (x86, x86_64, ppc64, ppc64le)		Instructions	32-bit 64-bit			
	For best results with R	PM package	uration Tool.						
	Deblan and Ubuntu Packages	DEB Package	Debian/Ubuntu (x86, x86_64, ppc64el)		Instructions	Mirror			
	For best results with D	EB package	s, use the Repositor	y Configu	aration Tool.	Accretive Networks			
						DigitalOcean - San Francisco, US			
						Jaleco.com - US East Coas			

1.2.2) Click Red Hat, Fedora, and CentOS Packages

- 1.3) Click Applications / Terminal
- 1.4) Type yum -y localinstall maria*
- 1.5) Type yum update
- 1.6) Type yum -y install mariadb-server mariadb php php-mysqlnd
- 1.7 Type "rpm -qa httpd php mariadb-server
- 1.8) Change httpd for active
 - 1.8.1) Type systemctl status httpd
 - 1.8.2) Type systemctl restart httpd
 - 1.8.3) Type systemctl enable httpd

root@localhost:~	-		×
File Edit View Search Terminal Help			
 httpd.service - The Apache HTTP Server Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; : disabled) 	vendor	pres	et
Active: active (running) since Wed 2019-07-17 16:30:04 PDT; 3h 5 Docs: man:httpd(8) man:apachectl(8)	34min ao	10	
Process: 9896 ExecReload=/usr/sbin/httpd \$0PTIONS -k graceful (co atus=0/SUCCESS)	de=exit	ted,	st
Main PID: 7762 (httpd) Status: "Total requests: 0; Current requests/sec: 0; Current tra	affic:	ΘE	3/s
Tasks: 7			
CGroup: /system.slice/httpd.service			
-7762 /usr/sbin/httpd -DFOREGROUND			
—9903 /usr/sbin/httpd -DFOREGROUND			
-9906 /usr/sbin/httpd -DFOREGROUND			
-9907 /usr/sbin/httpd -DFOREGROUND			
9908 /usr/spin/nttpa -DFOREGROUND			
-9909 /usr/spin/httpd -DFOREGROUND			

1.9) Change mariadb for active

1.9.1) Type systemctl status mariadb

1.9.2) Type systemctl enable mariadb

1.9.3) Type systemctl restart mariadb

root@localhost:~	-		×
File Edit View Search Terminal Help			
 mariadb.service - MariaDB database server Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; ve et: disabled) 	ndor	pr	es
Active: active (running) since Wed 2019-07-17 16:30:05 PDT; 3h 44min Process: 7555 ExecStartPost=/usr/libexec/mariadb-wait-ready \$MAINPID ted, status=0/SUCCESS)	ago (cod	le=e	xi
<pre>Process: 7478 ExecStartPre=/usr/libexec/mariadb-prepare-db-dir %n (co , status=0/SUCCESS) Main DID: 7552 (muscld cofe)</pre>	de=e	xit	ed
Tasks: 20			- 1
CGroup: /system.slice/mariadb.service -7553 /bin/sh /usr/bin/mysqld_safebasedir=/usr -7779 /usr/libexec/mysqldbasedir=/usrdatadir=/var/lib	/mys	ql.	

1.10) Change firewall

1

1.10.1) Type firewall-config

1.10.2) Change configuration from runtime to permanent

1.10.3) Click mysql in public zone

[1	irewall Configuration	_ = ×
File Options View	Help			
✓ Active Bindings	Configuration:	Permanent 👻		
Connections	Zones S	ervices IP	Sets	
Palm Spring (ens32) Default Zone: public	A firewalld zon	e defines the l	evel of trust for network connections, inter	faces and source addresses
virbr0 (virbr0) Default Zone: public	bound to the zo icmp filters and	one. The zone rich rules. The	combines services, ports, protocols, masqu zone can be bound to interfaces and sour	Jerading, port/packet forwarding, ice addresses.
San Bernardino (eno. Default Zone: public	block		Services Ports Prot	ocols Source Ports
Interfaces	dmz		Here you can define which services are tru	usted in the zone. Trusted
Sources	arop		services are accessible from all hosts and	networks that can reach the
	bome		machine from connections, interfaces and	sources bound to this zone.
	internal		Service	
	public		mssal	
	trusted		ms-wbt	
	work		murmur	
			mysql	
			nfs	
			nfs3	
			nmea-0183	
			nrpe nrpe	
li			ntp	
Change Zone		- 4	- 0000V/00	
Connection to firewalld	established. Chan	ges applied.		
Default Zone: public Lo	og Denied: off Pa	nic Mode: disa	bled Automatic Helpers: system (on) Lo	ckdown: disabled

1.10.4) Click reload firewalld in options

- 1.8) Type cd /var/www/html/
- 1.9) Type touch phpinfo.php
- 1.10) Type vi phpinfo.php
 - 1.22) Type <?php phpinfo(); ?>

				root@localhost:/var/www/html	-	×
File Edi	t View	Search	Terminal	Help		
php</td <td>phpinf</td> <td>o();</td> <td>?></td> <td></td> <td></td> <td></td>	phpinf	o();	?>			
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
~						- 8
"phpinf	o.php"	1L, 200	:			

2) Web hard

2.1) Start the Linux operating systems (Server B), by clicking Applications / Firefox web browser.

2.2) Type https://sourceforge.net/projects/ajaxplorer/files/pydio/stable-channel/6.0.2/

	Pydlo -	Browse /pydio/stable-	channel/6.0.2 at	SourceForge.net	- Mozilla Fire	fox	-		×
Pydio - Browse /pydio/stal ×	< +								
< → ୯ ଘ	①	eforge.net/projects/aja:	xplorer/files/pydio	/stable-channel/	5.0.2/	🗢	☆ III\	Ð	=
SOURCE FORG	SE <					Resources	Menu		
	-	③ 3. Start Conver	ting	PDF Co	nverter Hub	D LEARN MORE			_
1 (D					Advertisement - Repor		Advertisement		_
Formerly AJ Brought to y	io jaXplorer, file sharing	platform for the ente	rprise			∞	Website Customer Service		
Summary Files	Reviews	Support	Wiki	News	Code	Email, Pho Start Your	ne, and Live Chat Ava Site!	ilable.	
Download Latest Ve Latest Stable 7.0.0 (81.	ersion 8 kB) Ge	t Updates			>		OPEN	tisement - Re	spor
Home / pydio / stable-chann	el / 6.0.2		ei 🏠	Deverteed	- /)A/I- 🌨	Recomme	nded Projects		
J Parent folder			3120 🗢	Download	7 WEEK 🛥	est uplover	eXtplorer File Mana eXtplorer is a PHP-bas	ger led File	
pydio-core-6.0.2.tar.gz		2014-12-16	11.9 MB	0	Ø	Get	atest undates abo		
pydio-core-6.0.2.zip		2014-12-16	13.9 MB	0	\bigcirc	Ope	ferences and New	5	
pydio-core-upgrade-6.0.1-6.0	0.2.html	2014-12-16	874 Bytes	0	Ø		Sign Up		
pydio-core-upgrade-6.0.1-6.0	0.2.zip	2014-12-16	21.2 kB	0	Ì		No. Thank you		

2.2.1) Click to download pydio-core-6.0.2.tar.gz

2.3) Click Applications / Terminal

- 2.4) Type cd /var/www/html/
- 2.5) Type mv /root/Downloads/pydio-core-6.0.2.tar.gz .
- 2.6) Type tar xfz pydio-core-6.0.2.tar.gz
- 2.7) Type mv /pydio-core-6.0.2 webhard
- 2.8) Type chmod 707 webhard
- 2.9) Type chown -R apache.apache webhard
- 2.10) Type yum -y --skip-broken install php-*
- 2.11) Type yum -y install epel-release
- 2.12) Type yum -y install php-mcrypt
- 2.13) Type vi /etc/httpd/conf/httpd.conf
 - 2.13.1) Type :set number
 - 2.13.2) Change from AllowOverride None to AllowOverride All around 151

columns

	root@localhost:/var/www/html _ 🗆 🖛 🗙	
File	dit View Search Terminal Help	
	8 # It can be "All", "None", or any combination of the keywords:	in.
	9 # Options FileInfo AuthConfig Limit	
	• # · · · · · · · · · · · · · · · · · ·	
	1 AllowOverride All	
	2	
	3 #	
	4 # Controls who can get stuff from this server.	
	5 #	
	6 Require all granted	
	7	
	8	
	9 #	
	Ø # DirectoryIndex: sets the file that Apache will serve if a directory	
	1 # is requested.	
	2 #	
	3 <ifmodule dir_module=""></ifmodule>	
	4 DirectoryIndex index.html	
	5	
	6	
	7 #	
	8 # The following lines prevent .htaccess and .htpasswd files from being	
	9 # viewed by Web clients.	
	⊙ #	

2.14) Type vi /etc/php.ini

2.14.1) Type :set number

- 2.14.2) Change from max_execution_time = 30 to max_execution_time = 300 - around 384 columns
- 2.14.3) Change from post_max_size = 8M to post_max_size = 100M around 672 columns
- 2.14.4) Change from upload_max_filesize = 2M to upload_max_filesize = 100M

- around 800 columns



2.15) Type cd /var/www/html/webhard/data/cache/

2.16) rm -f plugin*

2.17) Change httpd for active

2.17.1) systemctl status httpd

2.17.2) systemctl restart httpd

2.17.3) systemctl enable httpd

root@localhost:~	-		×
File Edit View Search Terminal Help			
<pre>httpd.service - The Apache HTTP Server Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vend disabled) Active: active (running) since Wed 2019-07-17 16:30:04 PDT; 3h 54min Docs: man:httpd(8) man:apachectl(8)</pre>	or p ago	pres o	et
Process: 9896 ExecReload=/usr/sbin/httpd \$OPTIONS -k graceful (code=e: atus=0/SUCCESS) Main PID: 7762 (httpd) Status: "Total requests: 0; Current requests/sec: 0; Current traffic	×ite :	ed, 0В	st /s
ec" Tasks: 7 CGroup: /system.slice/httpd.service -7762 /usr/sbin/httpd -DFOREGROUND -9903 /usr/sbin/httpd -DFOREGROUND -9906 /usr/sbin/httpd -DFOREGROUND -9908 /usr/sbin/httpd -DFOREGROUND -9909 /usr/sbin/httpd -DFOREGROUND -9909 /usr/sbin/httpd -DFOREGROUND -9910 /usr/sbin/httpd -DFOREGROUND			

Configurations of Linux Client:

3) Install Web hard

3.1) Start the Linux operating systems (Linux Client), by clicking Applications / Firefox web browser.

- 3.2) Type 10.1.1.20/webhard
 - 3.2.1) Click pydio, English, Start wizard
 - 3.2.2) CSUSB in id, 1234 in password
 - 3.2.3) Admin access admin in admin login, admin in admin display name,

12345678 in admin password

- 3.2.4) Global options English in default language
- 3.2.5) Configurations storage Click Database system in stroage type, xeDB in database, xeUser in user, 1234 in password click try connecting to the database
- 3.2.6) Add some users Type "CSUSB in login, admin@csusb.com in user email,

User in display name, 1234 in password" then click install pydio now



3. File Transfer Protocol (FTP) Server – Configurations

Each machine requires a different process in order to be built. Here are the necessary components for each server machine and client machine.

Configurations of Server B:

1) FTP Server

- 1.1) Start the Linux operating systems (Server B), by clicking Applications / Terminal.
- 1.2) Type yum -y install vsftpd
- 1.3) Type cd /var/ftp/
- 1.4) Type cd /pub/
- 1.5) Type cp /boot/vmlinuz-3* file1
- 1.6) Type vi /etc/vsftpd/vsftpd.conf/
 - 1.6.1) Type :set number
 - 1.6.1) Change from #write_enable=YES to write_enable=YES around 19 columns
 - 1.6.2) Change from #anon_upload_enable=YES to anon_upload_enable= YES
 - around 29 columns
 - 1.6.3) Change #anon_mkdir_write_enable=Yes to anon_mkdir_write_enable=Yes

	root@localhost:/var/ftp	—		×
File	Edit View Search Terminal Help			
	25 Uncomment this to allow the anonymous FTP user to upload file nly	ès.	Thi	s o
	<pre>26 # has an effect if the above global write enable is activated. will</pre>	Als	0,	you
	27 # obviously need to create a directory writable by the FTP user	~ -		
	<pre>28 # When SELinux is enforcing check for SE bool allow_ftpd_anon_v ow_ftpd_full_access</pre>	vrit	е,	all
	<pre>29 anon_upload_enable=YES</pre>			
	30 #			
	31 # Uncomment this if you want the anonymous FTP user to be able	to	crea	ate
	32 # new directories.			
	33 anon_mkdir_write_enable=YES			
	34 #			
	35 # Activate directory messages - messages given to remote users	whe	n ti	hey
	36 # go into a certain directory.			
	37 dirmessage_enable=YES			
	38 #			
	39 # Activate logging of uploads/downloads.			
	40 xferlog_enable=YES			
	41 #			
	42 # Make sure PORT transfer connections originate from port 20 (1	ftp-	data	a).
	43 connect from port 20=YES			
	44 #			

- around 33 columns

1.7) Type chown ftp.ftp /var/ftp/pub/

1.8) Change firewall

1.8.1) Type firewall-config

1.8.2) Change configuration from runtime to permanent

1.8.3) Click ftp in public zone

Firewall Configuration _ 🗆 🖛 🗙										
File Options View	ile Options View Help									
✓ Active Bindings	Configuration: Permanent	~								
Connections	Zones Services	PSets								
Palm Spring (ens32) Default Zone: public San Bernardino (eno. Default Zone: public	A firewalld zone defines the bound to the zone. The zon icmp filters and rich rules. T	e level of trust for network connections, interfaces and source addresses e combines services, ports, protocols, masquerading, port/packet forwarding, 'he zone can be bound to interfaces and source addresses.								
Virbr0 (virbr0) Default Zone: public	block	Services Ports Protocols Source Ports								
Interfaces Sources	dmz drop external home internal public trusted work	Here you can define which services are trusted in the zone. Trusted services are accessible from all hosts and networks that can reach the machine from connections, interfaces and sources bound to this zone. Service elasticsearch freeipa-ldap freeipa-ldaps freeipa-trust ftp ganglia-client ganglia-master oit								
Change Zone	+ 🖹 — Ġ	gre								
Connection to firewalld e Default Zone: public Lo	ionnection to firewalld established.									

1.9) Change vsftpd for active

1.9.1) Type systemctl status vsftpd

1.9.2) Type systemctl restart vsftpd

1.9.3) Type systemctl enable vsftpd

		re	ot@localhost:/va	r/ftp/pub		_		×
File Edit Vi	ew Search Te	rminal He	lp					
<pre>vsftpd.se Loaded: t: disabled Active: Process: status=0/S Main PID: Tasks: CGroup:</pre>	rvice - Vsft loaded (/usr) active (runn 9977 ExecSta JCCESS) 9978 (vsftpd 1 /system.slic	pd ftp d /lib/sys ing) sin rt=/usr/) e/vsftpd sbin/vsf	aemon temd/system/v ce Fri 2019-0 sbin/vsftpd / service	sftpd.service 7-19 00:11:15 etc/vsftpd/vs	; enabled; ve PDT; 8s ago ftpd.conf (co	ndor de=e:	pre xite	se d,

Configurations of Linux Client.

2) FTP Linux Client

2.1) Start the Linux operating systems (Linux Client), by clicking Applications / Terminal.

2.2) Type yum -y install epel-release

2.3) Type yum -y install filezilla

2.4) Type filezilla

2.4.1) Type 10.1.1.20 in host

2.4.2) Type anonymous in username

2.4.3) Type 1234 in password

2.4.4) Type 21 in port

2.4.5) Click quickconnect

			anonymous@192	2.168.1	.11.100 -	FileZ	illa			-	•	×
File Edit Vie	w Transfer	Server Book	kmarks Help									
: 😹 💌 📰		90 🦗 🙀	* 🗈 📯 😤	*								
Host: 10.1.1.	20 User	name: anon	ymou Password: •	•••	Port:	21	Qu	lickconnect	-			
Command: LIST Response: 150 Response: 226 Status: Direc	Here comes th Directory send ctory listing suc	e directory list OK. :cessful	ing.									
Local site: /			-	R	emote sit	e: 📝	,					-
20 1					►							
Filename 🔨	Filesize	Filetype	Last modified	F	ilename ·	F	ilesize	Filetype	Last modified	Permi	ssion	s Ow
📁 bin		Directory	07/19/2019 03:									
📁 boot		Directory	06/20/2019 12:		pub			Directory	10/30/2018	drwxr-	xr-x	14 5
📁 dev		Directory	07/19/2019 03:									
📁 etc		Directory	07/19/2019 03:									
📁 home		Directory	04/11/2018 12:									
📁 lib		Directory	06/20/2019 12:									
19 directories				1	directory							
Server/Local file	e D	rectior Remot	e file		Size Prio	rity	Status					
Queued files	Failed transfe	rs Success	ful transfers									
	~							F	Queue: em	pty		•
	-	-	-									

4. Firewall - Configurations

Each machine requires a different process in order to be built. Here are the necessary components for each server machine and client machine.

Configurations of Server A:

1) Network setting

- 1.1) Start the Linux operating systems (Server A), by clicking Applications / Terminal.
- 1.2) Type cd /etc/sysconfig/network-scripts/
- 1.3) Type vi ifcfg-eno16777736
 - 1.3.1) Type :set number

1.3.2) Change from BOOTPROTO="dhcp" to BOOTPROTO=none - around 3

columns



1.4) Change httpd for active

1.4.1) Type systemctl status httpd

1.4.2) Type systemctl restart network

1.4.3) Type systemctl enable network

root@localhost:/etc/sysconfig/network-scripts		×
File Edit View Search Terminal Help		
 network.service - LSB: Bring up/down networking Loaded: loaded (/etc/rc.d/init.d/network; bad; vendor preset: disabled Active: active (exited) since Thu 2019-07-18 23:59:07 PDT; 1h 5min ago Docs: man:systemd-sysv-generator(8) Tasks: 0 	d) c	

1.5) Type vi /etc/sysconfig/selinux

1.5.1) Type :set number

1.5.2) Change from SELINUX=enforcing to SELINUX=disabled – around 7

columns

	root@localhost:/etc/sysconfig/network-scripts _ 🛛 🗙
File	Edit View Search Terminal Help
	<pre>1 2 # This file controls the state of SELinux on the system. 2 # SELINUX= can take one of these three values: 4 # enforcing - SELinux security policy is enforced. 5 # permissive - SELinux prints warnings instead of enforcing. 6 # disabled - No SELinux policy is loaded. 7 SELINUX=disabled 8 # SELINUXTYPE= can take one of these two values: 9 # targeted - Targeted processes are protected, 10 # minimum - Modification of targeted policy. Only selected processes are protected. 11 # mls - Multi Level Security protection. 12 SELINUXTYPE=targeted 13 14</pre>
~	
~	
~	
~	
~	
~	
~	
:set	number

2) First IP address

2.1) Virtual machine settings

2.1.1) Click network adapter

2.1.2) Click nat: used to share the host's IP address

rdware Options		
Device Memory Processors Hard Disk (SCSI) Co/DVD (IDE) Network Adapter Network Adapter 2 Display	Summary 2 GB 1 80 GB Using file C:\CentOS\CentOS NAT Bridged (Automatic) Auto detect	Device status Connected Connect at power on Network connection Bridged: Connected directly to the physical network Replicate physical network connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network VMnet0 LAN segment: Advanced

- 2.2) Click Applications / Terminal.
- 2.3) Type nmtui edit Wired connection 1
 - 2.3.1) 10.1.1.1/24 in addresses
 - 2.3.2) 10.1.1.1 in gateway
 - 2.3.3) 8.8.8.8 in DNS servers
 - 2.3.4) Click ok
 - 2.3.5) reboot

	root@localhost:~	-		×
File	Edit View Search Terminal Help			
	Edit Connection Profile name Wired connection 1 Device 00:0C:29:BB:78:11 (eno16777736)		Ť	
	= ETHERNET	<show></show>		
	<pre>- IPv4 CONFIGURATION <manual> Addresses</manual></pre>	<hide></hide>		
	Routing (No custom routes) <edit> [] Never use this network for default route [] Ignore automatically obtained routes [] Ignore automatically obtained DNS parameters</edit>		Ţ	

- 3) Second IP address
 - 3.2) Virtual machine settings
 - 3.2.1) Click add
 - 3.2.2) Click network adapter
 - 3.2.3) Click bridged: connected directly to the physical network

Building a secure network test environment using virtual machines

Virtual Machine Settings			\times
Hardware Options			
Device Memory Hard Disk (SCSI) Hard Disk (SCSI) Display Network Adapter 2 Display	Summary 2 GB 1 80 GB UAT Bridged (Automatic) Auto detect Auto detect	Device status Connect at power on Connect at power on Network connection Bridged: Connected directly to the physical network Connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network VMnet0 LAN segment: LAN Segments	<
		OK Cancel	Help

3.3) Click Applications / Terminal.

3.4) Type nmtui edit Wired connection 2

2.3.1) 192.168.111.100/24 in addresses

2.3.2) 192.168.111.2 in gateway

2.3.3) 192.168.111.2 in DNS servers

3.11) Click ok

3.12) reboot

	root@localhost:~	_		×
File	e Edit View Search Terminal Help			
File	Edit View Search Terminal Help Edit Connection 2 Device 00:0C:29:BB:78:1B (ens32) = ETHERNET = IPv4 CONFIGURATION <manual> Addresses 192.168.111.100/24 <add> Gateway 192.168.111.2 DNS servers 192.168.111.2 Search domains <add></add></add></manual>	<show> <hide></hide></show>	Ť	
	Routing (No custom routes) <edit> [] Never use this network for default route [] Ignore automatically obtained routes [] Ignore automatically obtained DNS parameters</edit>		Ļ	

4) iptables

4.1) Click Applications / Terminal.

4.2) Type vi /etc/sysctl.conf

4.2.1) Type :set number

4.2.2) Type net.ipv4.ip_forward = 1 - around 11 columns

```
root@localhost:~
                                                                                                                                                     ×
File
         Edit
                   View Search Terminal Help
                   sysctl settings are defined through files in
/usr/lib/sysctl.d/, /run/sysctl.d/, and /etc/sysctl.d/.
            1
2
               #
            з
                  Vendors settings live in /usr/lib/sysctl.d/.
To override a whole file, create a new file with the same in
/etc/sysctl.d/ and put new settings there. To override
only specific settings, add a file with a lexically later
name in /etc/sysctl.d/ and put new settings there.
           4
5
               #
#
            6
               #
            7
               #
            8
               #
           9
               #
              # For more information, see sysctl.conf(5) and sysctl.d(5).
          10
          11 net.ipv4.ip_forward = 1
:set number
```

4.3) Type echo 1 > /proc/sys/net/ipv4/ip_forward

4.4) Change iptables policy

4.4.1) Type iptables --policy FORWARD DROP

4.4.2) Type iptables --policy INPUT DROP

4.4.3) Type iptables --policy OUTPUT DROP

4.5) Iptable policy specifications

4.5.1) iptables --append INPUT --in-interface ens32 --source 10.1.1.0/24 --match

state --state NEW, ESTABLISHED --jump ACCEPT

- 4.5.2) iptables --append OUTPUT --out-interface ens32 --destination 10.1.1.0/24 --match state --state NEW,ESTABLISHED --jump ACCEPT
- 4.5.3) iptables --append FORWARD --in-interface ens32 --source 10.1.1.0/24 -destination 0.0.0.0/0 --match state --state NEW,ESTABLISHED --jump ACCEPT
- 4.5.4) iptables --append FORWARD --in-interface eno16777736 destination 10.1.1.0/24 --match state --state NEW,ESTABLISHED --jump ACCEPT
- 4.5.5) iptables --table nat --append POSTROUTING --out-interface eno16777736 --jump MASQUERADE
- 4.5.6) service iptable save
- 4.6) Change firewall
 - 4.6.1) Type firewall-config
 - 4.6.2) Change configuration from runtime to permanent
 - 4.6.3) Click masquerading then masquerade zone
 - 4.6.4) Click reload firewalld in options



5) iptables for http

- 5.1) Click Applications / Terminal.
- 5.2) Type iptables --table nat --append PERROUTING --proto tcp --in-interface eno16777736 --dport 80 --jump DNAT --to-destination 10.1.1.20
- 5.4) Type service iptable save

6) iptables for ftp

- 6.1) Click Applications / Terminal.
- 6.2) iptables --table nat --append PERROUTING --proto tcp --in-interface eno16777736

--dport 21 --jump DNAT --to-destination 10.1.1.20

6.3) service iptable save

Configurations of Server B:

7) Network setting

- 7.1) Start the Linux operating systems (Server B), by clicking Applications / Terminal.
- 7.3) Type cd /etc/sysconfig/network-scripts/
- 7.4) Type vi ifcfg-eno16777728
 - 7.4.1) Type :set number

7.4.1) Change from BOOTPROTO="dhcp" to BOOTPROTO=none

	root@localhost:/etc/sysconfig/network-scripts	-	×
File	Edit View Search Terminal Help		
	1 HWADDR="00:0C:29:81:75:D1"		
	2 PE="Ethernet"		- 8
	3 BOOTPROTO=none		- 8
	4 IPADDR=10.1.1.20 5 NETMACK-255 255 0		- 8
	6 GATEWAY=10 1 1 1		- 8
	7 DNS1=8.8.8.8		- 8
	8 DEFROUTE="yes"		- 8
	9 PEERDNS="yes"		- 8
	10 PEERROUTES="yes"		- 8
	11 IPV4_FAILURE_FATAL="no"		- 8
	12 IPV6INIT="yes"		- 8
	<pre>13 IPV6_AUTOCONF="yes"</pre>		- 8
	14 IPV6_DEFROUTE="yes"		- 8
	15 IPV6_PEERDNS="yes"		- 8
	10 IPV6_PEERROUTES="yes"		- 8
	1/ 1FV0_FAILORE_FAILE HO		- 8
	19 UUTD="60e2308c-e9e0-4c47-b4cd-73e90e91f044"		- 8
	20 ONBOOT="ves"		- 8
	21 ZONE=		- 8
~	—		- 8
~			- 8
I	NSERT		

7.5) Change network for active

7.5.1) systemctl status network

7.5.2) systemctl restart network

7.5.3) systemctl enable network

root@localhost:~	-		×
File Edit View Search Terminal Help			
 network.service - LSB: Bring up/down networking Loaded: loaded (/etc/rc.d/init.d/network; bad; vendor preset: disab Active: active (exited) since Fri 2019-07-19 16:18:36 PDT; 1h 15min Docs: man:systemd-sysv-generator(8) Process: 7129 ExecStart=/etc/rc.d/init.d/network start (code=exited, SUCCESS) Tasks: 0 	led) ago sta	tus=	:0/

7.6) Type vi /etc/sysconfig/selinux

7.6.1) Type :set number

7.6.2) Change from SELINUX=enforcing to SELINUX=disabled - around 7

columns

	root@localhost:/etc/sysconfig/network-scripts ×
File	Edit View Search Terminal Help
~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~	<pre>1 2 # This file controls the state of SELinux on the system. 3 # SELINUX= can take one of these three values: 4 # enforcing - SELinux security policy is enforced. 5 # permissive - SELinux policy is loaded. 6 # disabled - No SELinux policy is loaded. 7 SELINUX=disabled 8 # SELINUXTYPE= can take one of these two values: 9 # targeted - Targeted processes are protected, 10 # minimum - Modification of targeted policy. Only selected processes are protected. 11 mls - Multi Level Security protection. 12 SELINUXTYPE=targeted 14 </pre>
:set	number

8) IP address

8.1) Virtual machine settings

8.2) Click network adapter

8.3) Click bridged: connected directly to the physical network

Virtual Machine Settings	×
Hardware Options	
Device Summary Memory 2 GB Hard Disk (SCSI) 40 GB OC/DVD (DE) Using file C:\CentOS\CentOS Network Adapter Bridged (Automatic) Display Auto detect Add Remove	Device status Connected Connect at power on Network connection Bridged: Connected directly to the physical network Replicate physical network connection state NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network Mnet0 UAN segment: LAN Segments Advanced
	OK Cancel Help

- 8.4) Click Applications / Terminal.
- 8.5) Type nmtui edit eno16777728

8.5.1) 10.1.1.20/24 in addresses

8.5.2) 10.1.1.1 in gateway

8.5.3) 8.8.8.8 in DNS servers

8.5.4) Click ok

8.5.5) reboot

	root@localhost:~ _ □					
File	e Edit View Search Terminal Help					
	Edit Connection Profile name Device Device Addresses 10.1.1.20/24 <add> Gateway DNS servers 8.8.8 <add> Search domains Add> Routing (No custom routes) <edit> [] Never use this network for default route [] Ignore automatically obtained routes [] Ignore automatically obtained DNS parameters</edit></add></add>	<show> <hide></hide></show>	Ť ■			

Configurations of Linux Client:

9) Network setting

9.1) Start the Linux operating systems (Linux Client), by clicking Applications / Terminal.

9.2) Type cd /etc/sysconfig/network-scripts/

9.3) Type vi ifcfg-eno16777736

9.3.1) Type :set number

9.3.1) Change from BOOTPROTO="dhcp" to BOOTPROTO=none – around 2

columns

				root@l	ocalhos	:/etc/sysconf	ig/netwo	ork-scripts	_	×
File	Edit	View	Search	Terminal	Help					
	1	YPE=E	thernet	t						
	2	BOOTPR	OT0=nor	ne						
	3	DEFROU	TE=yes							
	4	IPV4_F	AILURE	FATAL=nd	>					
	5	IPV6IN	IIT=yes							
	6	IPV6_A	UTOCONF	=yes						
	7	IPV6_D	EFROUTE	=yes						
	8	IPV6_F	AILURE	FATAL=no						
	9	NAME=I	nformat	tion						
	10	UUID=b	18c4053	3-77d1-40	583 - bd	71-79ed917	66459			
	11	ONBOOT	=yes							
	12	GATEWA	Y0=10.1	1.1.1						
	13	DNS1=8	.8.8.8							
	14	HWADDR	=00:00:	29:88:34	1:12					
	15	PROXY	METHOD=	none						
	16	BROWSE	R_ONLY=	=no						
	1/	IPADDR	=10.1.1	1.10						
	18	PREFIX	=24							
	19	GATEWA	Y=10.1.	1.1						
~										
~										
~										
:set	nun	ber								

9.4) Change network for active

9.4.1) systemctl status network

9.4.2) systemctl restart network

9.4.3) systemctl enable network

root@localhost:~ _		×
File Edit View Search Terminal Help		
[root@localhost ~]# systemctl status network		
network.service - LSB: Bring up/down networking		
Loaded: loaded (/etc/rc.d/init.d/network; bad; vendor preset: disabled)	
Active: active (exited) since Sat 2019-07-20 03:04:14 EDT; 2min 22s ag	2	
Docs: man:systemd-sysv-generator(8)		
Process: 10888 ExecStop=/etc/rc.d/init.d/network stop (code=exited, sta	tus=	0/S
UCCESS)		
Process: 11087 ExecStart=/etc/rc.d/init.d/network start (code=exited, s	tatu	s=0
/SUCCESS)		

9.5) Type vi /etc/sysconfig/selinux

9.5.1) Type :set number

9.5.2) Change from SELINUX=enforcing to SELINUX=disabled



10) IP address

10.1) Virtual machine settings

10.2) Click network adapter

Virtual Machine Setting	s	× ×
Hardware Options		
Device Memory Processors CD/DVD (IDE) Sound Card Printer Display	Summary 2 GB 1 40 GB Auto detect Bridged (Automatic) Present Auto detect Present Auto detect Present Auto detect	Device status Connect at power on Network connection Bidged: Connected directly to the physical network C Replicate physical network connection state NAT: Used to share the host's IP address Lots-only: A private network shared with the host C custom: Specific virtual network Minet0 C LAN segment: LAN Segments Advanced
		Cancer Help

10.3) Click bridged: connected directly to the physical network

10.2) Click Applications / Terminal

10.3) Type nmtui edit eno16777736

10.3.1) 10.1.1.10/24 in addresses

10.3.2) 10.1.1.1 in gateway

10.3.3) 8.8.8.8 in DNS servers

10.3.4) Click ok

10.3.5) reboot

root@localhost:~	-		×
File Edit View Search Terminal Help			
Edit Connection Profile name Device eno16777736 00:0C:29:B8:34:12 (eno16777736) - ETHERNET IO.1.1.10/24 Addresses <remove> <add> Gateway IO.1.1.1 DNS servers 8.8.8.8 <remove> <add> Search domains <add> Routing (No custom routes) <edit> [] Never use this network for default route [] Ignore automatically obtained routes [] Ignore automatically obtained DNS parameters</edit></add></add></remove></add></remove>	<show> <hide></hide></show>	Ť	

Configurations of Window Client:

11) IP address

11.1) Virtual machine settings

11.1.1) Click network adapter

11.1.2) Click nat: used to share the host's IP address

Building a secure network test environment using virtual machines

rtual Machine Settings	5	×
Ardware Options Davice Memory Hard Disk (SCS1) Co/DvD (SATA) Co/DvD (SATA) Display	Summary 2 GB 1 20 GB Auto detect NAT Auto detect	Device status Connected Connect at power on Network connection Bridged: Connected directly to the physical network Replicate physical network connection state NAT: Used to share the host's IP address Custom: Specific virtual network VMnet0 LAN segment: LAN Segments
		OK Cancel Help

11.2) Network connections

11.2.1) Click Ethernet 0 / properties

11.2.2) Click Internet Protocol Version 4 (TCP/IPv4)

11.2.3) Click obtain an IP address automatically

11.2.4) Click use the following DNS server address automatically

11.2.5) Type 192.168.111.100

11.2.6) Click ok

Internet Protocol Version 4 (TCP/IPv4) Properties
General Alternate Configuration	
You can get IP settings assigned automatic this capability. Otherwise, you need to ask for the appropriate IP settings.	cally if your network supports your network administrator
Obtain an IP address automatically	
O Use the following IP address:	
IP address:	
Subnet mask:	
Default gateway:	
Obtain DNS server address automatic	ally
Use the following DNS server address	es:
Preferred DNS server: 1	92.168.111.100
Alternate DNS server:	· · ·
Validate settings upon exit	Advanced
	OK Cancel

12) Install FTP Client

12.1) Click Internet explorer

12.2) Type http://www.filezilla-project.org

- 12.3) Click download
- 12.4) Click download Filezilla client

	lla-project.org/download.php?type=client 🔎 - 🔒 🔿	Download FileZilla Client fo ×
E Fil	eZilla	î
Home		
Features Screenshots Download Documentation FileZilla Pro	The Best FTP Solution	
FileZilla Server	The latest stable version of FileZilla Client is 3,43,0	
Community Forum Project page	Please select the file appropriate for your platform below. Windows (64bit) 🚝	
General FAQ Support Contact	Download FileZilla Client	
Privacy Policy Trademark Policy	This installer may include bundled offers. Check below for more options.	
Source code	The 64bit versions of Windows 7, 8, 8.1 and 10 are supported.	
Nightly builds Translations Version history Changelog	◇ More download options Other platforms:	
Issue tracker	Not what you are looking for?	~

13) Nmap

- 13.1) Click Internet explorer
- 13.2) Type https://nmap.org/download.html

13.3) Click download

13.4) Click nmap-7.70-setup.exe

	en e		
	//nmap.org/download.html 🔎 🗧 Download the Free Nmap S × 👔 🏠 🔅		
About/Contact	License, as noted in the copyright page.		
Site Search	Microsoft Windows binaries		
Sponsors: ARMIS ARMIS OT Security Best Practices Gartar Bertemen 2010	Image: Second		
	Linux RPM Source and Binaries		