Lab 7-Web Server Security

Dawn M Inman

CSC-432 Computer and Network Security

Professor Nick Merante

April 24, 2020

Abstract

This lab sets up the Apache WebServerVM with HTTPS going through the steps of installation, creating certificates and configuring the server for them, using .htaccess to password protect the web content and forwarding HTTP requests to the HTTPS address.

Keywords: Apache/2.3.4 (CentOS), CentOS 7, FirewallD, NAT, Kali Xfce, Proxmox, KVM, QEMU, PuTTY.

Lab 7-Web Server Security

A web server serves websites on the internet. It acts like a middleman between the server and client machines and can get information from a client and deliver it to the server. It is made up of two parts, both hardware and software. A virtual web server adds another layer to the software and networking sides of the server. The hardware is the computer that holds the software, files for the programs and data files. The software runs various internet services like HTTP or HTTPS, holds domain names, web pages, and ways to deliver content to the end user, at minimum. The software being used for running the web server is Proxmox for running the virtual part of the networking and Apache/2.4.6 (CentOS).

Apache/2.4.6 (CentOS) is an open source web server that creates, deploys and manages software. It was designed to be able to host at least one website using the HTTP language but has been added on so that extensions for HTTPS are being used for the WebServerVM. These are called modules and they can be turned on and off. The Apache servers can also distinguish between different web hosts that are on one machine. (MDN contributors, 2019) Apache is designed to run on Unix and Windows servers, so it is a cross-platform software. (Domantas,2020)

CentOS 7 is so named because it stands for Community ENTerprise Operating System. It is based on the Linux kernel, free and has been available since 2004. Red Hat Enterprise Linux is the origination of CentOS 7 so it is a compatible option when requiring Linux software. It is very popular with almost 30% of Linux web servers using it in 2011 and has been one of the most popular in hosting history. (CentOS Blog, 2020)

NAT stands for Network Address Translation. It allows an internal network (private network) to have one internet gateway. This gateway is the CentOS 7 router. The machines on the internal network can have different IP addresses inside the network but when going outside of the router it will appear as if there is only one IP address being used. (Bischoff, 2019)

Kali Xfce is a newer Kali release. It is on the same line of Kali environments that have been created for Penetration Testing. There is a new feature called "Kali Undercover" which can make the display of Kali look like Windows 10. This can happen quickly so it is a type of stealth feature meant for blending in when in public areas. (Abrams, 2019) Other new features include KaliNetHunter KeX for Android which can install a full Kali desktop via Android, upgrading the kernel, Git powered documentation and adding PowerShell. (Elwood, 2019)

Proxmox is also being used by the systems. Proxmox VE hypervisor is based on GNU/Linux (Debian) and is open source. It has a central web-based management that does not require more installation. (Cheng, 2014) Version 5.4 is built specifically on Debian 9.8 with a "specially modified Linux Kernel 4.15". (Proxmox, 2019) Proxmox is capable of two types of virtualization: OpenVZ and KVM. OpenVZ needs a patched Linux kernel so Linux guests are the only operating system type that can be created. In OpenVZ, the guests are called containers because they share the same architecture and kernel as the host operating system. (Cheng, 2014) KVM (Kernel-based Virtual Machine) is a modified Linux kernel built with the KVM module so that it can give hardware-assisted virtualization. Virtualization is performed by a software-based emulator (QEMU) which simulates the virtualized environment while KVM only exposes the /dev/kvm interface. (Cheng, 2014) "This converts Linux into a Type 1 (bare-metal) hypervisor." (What is KVM?, 2020) Then QEMU or the software-based emulator will create the virtual machines on top of KVM. (What is KVM? 2020) Proxmox VE is relatively simple to start working with but can be very in depth as Simon M.C. Cheng has authored a book called

Proxmox High Availability which goes into more detail when setting up a high availability virtual cluster. (Cheng, 2014)

PuTTY is an SSH client for Windows, Mac and Linux. It has a terminal window for access to the server used in this lab, the GNU/Linux server named chewy. (How to use PuTTY on Windows, 2020) SSH is a software package and means Secure Shell. It secures system administration and file transfers even though the networks are insecure. Tatu Ylonen is the inventor of SSH and OpenSSH which is an open source SSH program is based off of his free versions. (SSH(Secure Shell), 2020)

Objective

This labs purpose is to install security features on the WebServerVM. Installing HTTPS, creating certificates and configuring for them as well as updating the firewall to allow for the traffic and password protecting the site with .htaccess are the tasks. The final task is to forward the HTTP traffic to the HTTPS site so that the web server remains secure.

The computer that is being used is a 2011 HP Pavillion dv7, i7 quad core processor and 16GB RAM with Windows10Pro operating system. Google Chrome is the internet browser being used for connecting to ProxMox including the Router and Kali Linux and WebServerVM consoles. The Kali Linux VM then runs Fire Fox internet browser. The router and WebServerVM use FirewallD for a firewall and the Kali Linux VM used iptables.

Results and Analysis[1]

In order for encryption to be able to install the newest version possible, the yum package on the web server needs to be updated properly. To do that, type

```
yum clean all
```

The response from this says that the repodata is over two weeks old and asks if it should install yum-cron or run yum makecache fast. The decision is to run yum makecache fast

```
yum makecache fast
yum clean all (is run again, then)
yum install mod_ssl
y (when asked is this okay?)
```

The response says complete, so moving on to creating the certificates.

```
cd /etc/httpd/
mkdir ssl
```

The next command is all on one line, but here it needs to be on more than one because it is lengthy.

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/httpd/ssl/apache.key
        -out /etc/httpd/ssl/apache.crt
```

Next, the Web Server needs to be configured to use the certificate.

```
vi /etc/httpd/conf.d/ssl.conf
```

This is done by going into the configuration file and uncommenting the following lines to make sure they are read the configuration happens.

```
DocumentRoot “/var/www/html”
ServerName localhost:443
SSLCertificateFile /etc/httpd/ssl/apache.crt
SSLCertificateKeyFile /etc/httpd/ssl/apache.key
```

Restart the httpd service for activation of the certificate.

```
system restart httpd
```

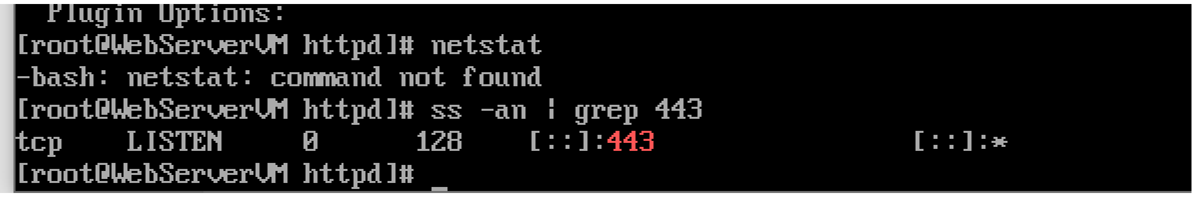
To verify the service is running, netstat needs to run to let us know with the command

netstat -an | grep 443

If this comes back with the return: command not found- that means that it is not recognizing the word netstat as a command. It is likely that it needs to be replaced by ss instead. The Web Server VM needed the following command, instead of the one above:

ss -an | grep 443

This gave the proper return of the device working properly.



```
  Plugin Options:
[root@WebServerVM httpd]# netstat
-bash: netstat: command not found
[root@WebServerVM httpd]# ss -an | grep 443
tcp    LISTEN     0      128    [::]:443                [::]:*
[root@WebServerVM httpd]# _
```

Figure 1 netstat shows https port is working properly

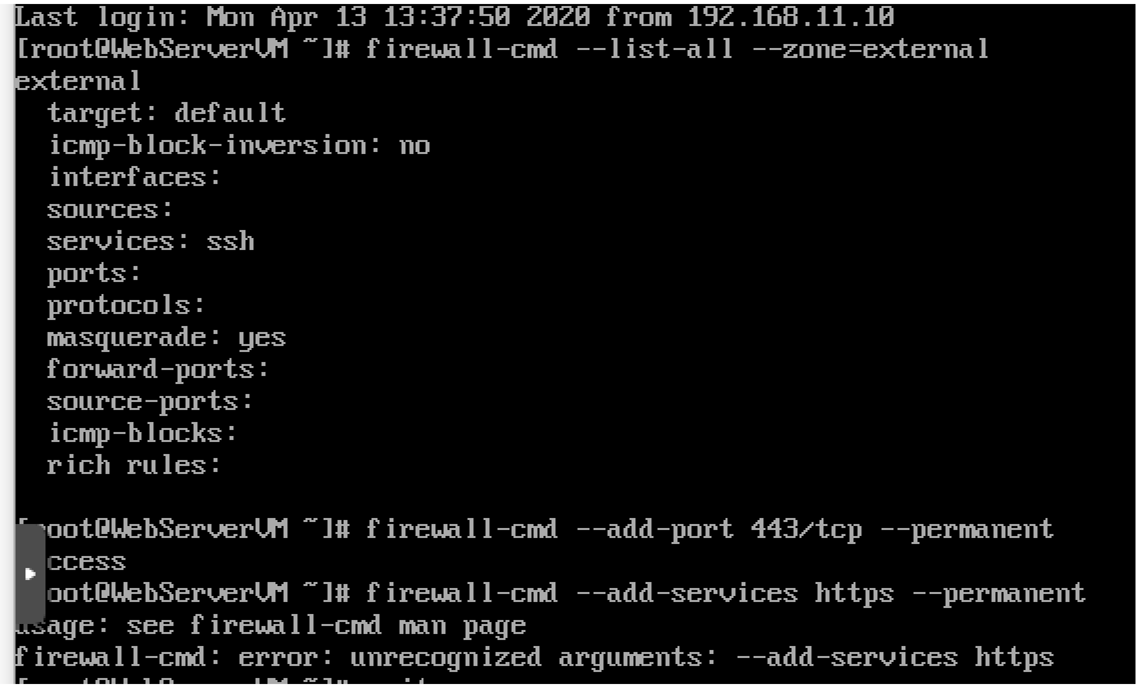
Next the host-based firewall needs to be updated to allow traffic for the HTTPS service which runs on port 443. First the port forwarding was written on the command line-all one line.

firewall-cmd –zone=external –add-forward-

port=port=443:proto=tcp:toport=443:toaddr=192.168.11.15 --permanent

Next the ports were added to each machine. First, on the WebServerVM, then on the routerVM.

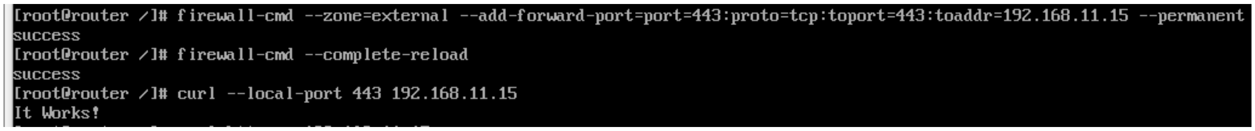
firewall-cmd –zone=external –add-port=443/tcp –permanent



```
Last login: Mon Apr 13 13:37:50 2020 from 192.168.11.10
[root@WebServerVM ~]# firewall-cmd --list-all --zone=external
external
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh
  ports:
  protocols:
  masquerade: yes
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

oot@WebServerVM ~]# firewall-cmd --add-port 443/tcp --permanent
ccess
oot@WebServerVM ~]# firewall-cmd --add-services https --permanent
sage: see firewall-cmd man page
firewall-cmd: error: unrecognized arguments: --add-services https
```

Figure 2 WebServerVM firewalld addition of HTTPS and port 443



```
[root@router /]# firewall-cmd --zone=external --add-forward-port=port=443:proto=tcp:toport=443:toaddr=192.168.11.15 --permanent
success
[root@router /]# firewall-cmd --complete-reload
success
[root@router /]# curl --local-port 443 192.168.11.15
It Works!
```

Figure 3 Router port forwarding to WebServerVM HTTPS port 443

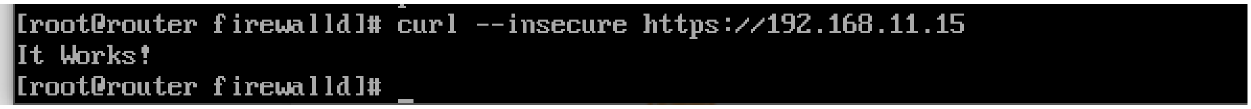
After BOTH the WebserverVM and the routerVM have the correct ports listed, then reload the settings:

firewall-cmd –complete-reload

To check to make sure the service is running properly, curl is used with the insecure option.

curl –insecure https://192.168.11.15

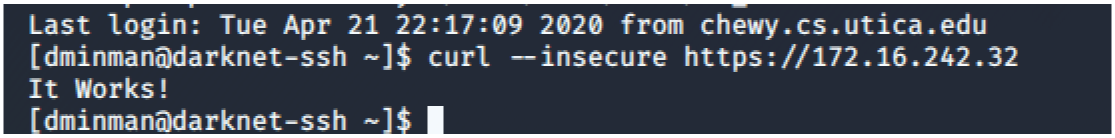
This means it’s up and working.



```
[root@router firewalld]# curl --insecure https://192.168.11.15
It Works!
[root@router firewalld]# _
```

Figure 4 WebServerVM HTTPS working from router

Type in the same into the darknet server to make sure it works:



```
Last login: Tue Apr 21 22:17:09 2020 from chewy.cs.utica.edu
[dminman@darknet-ssh ~]$ curl --insecure https://172.16.242.32
It Works!
[dminman@darknet-ssh ~]$ 
```

Figure 5 WebServerVM HTTPS working from darknet

.htaccess

The Apache webserver can use .htaccess files to change how it acts. Examples would be for password protection of web content and redirection of traffic from one web address to another, or service to another (in this case, HTTP to HTTPS).

First, password protection is going to be put onto the website. This has many short steps, but it's lengthy. In this section, what needs to be typed into the command prompt will be indented and comments will have a # in front of them so they are easily recognizable.

#Making the htaccess file. Touch is used to create the file but doesn't give the file any data inside it, just the file name.

```
touch /var/www/html/.htaccess
```

#Usernames and password credentials can be access with a credential file. This is where the authorized user-names and passwords are kept.

```
touch /etc/httpd/httpd-passwords
```

#Usernames and passwords need to be added to the password file. The utility, htpasswd, will be used to generate a hashed password so that during storage, the passwords are not readable. This creates added security for the users.

```
htpasswd /etc/httpd/httpd-passwords yourusername
```

#Here is where you put whatever username you would choose.

#The file needs to be verified to make sure everything adds to it correctly.

```
cat /etc/httpd/httpd-passwords
```

#The first file that was created needs to have content added so that it prompts for a username and password whenever the site is visited.

```
vi /var/www/html/.htaccess
```

#inside the file, add:

```
AuthUserFile  /etchttpd/httpd-passwords
AuthType      Basic
AuthName      restricted
Require       valid-user
```

#configure the web server to override the default settings with the .htaccess file. This is done by editing the Apache configuration file from “AllowOverride none” to “AllowOverride AuthConfig”. Start with:

```
vi /etc/httpd/conf/httpd.conf
```

#The “AllowOverride none” needs to be searched for. It is about at line 150.

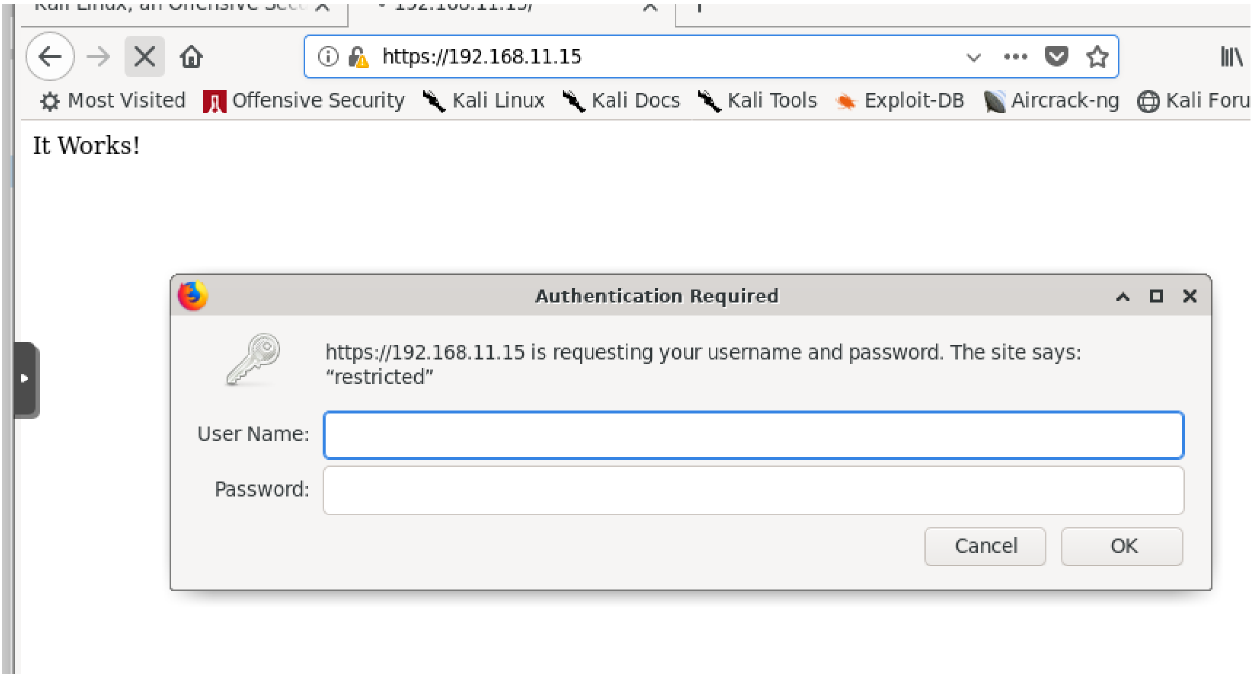
Change “AllowOverride none” to

```
AllowOverride AuthConfig
```

#Save and quit the file, then restart the Apache server with:

```
systemctl restart httpd.service
```

To make sure the service works, the web site was visited from the KaliVM. It prompts for the username and password, then goes to the “It Works!” page.



It Works!

Authentication Required

https://192.168.11.15 is requesting your username and password. The site says: “restricted”

User Name:

Password:

Figure 6 Authentication now required on the WebServerVM

Website redirection can be used to force the HTTP traffic that comes through to the WebServerVM to the HTTPS site. This action keeps all traffic on the WebServerVM secure and preauthorized. Forwarding to websites can also be useful as the student used this for small business purposes in the past, creating a free website on google sites, purchasing a domain name through godaddy and forwarding the traffic from the domain name to the google sites website. This created a very inexpensive website. For the case with the current WebServerVM, redirecting the traffic will create a secure connection even if the person connecting forgets to type in HTTPS and types in HTTP instead. To do this, a walk through of the process was found for an Apache redirect to HTTPS at Namecheap.com.

The first step to push the HTTP traffic to the HTTPS is to make these changes to the .htaccess file.

```
vi /var/www/html/.htaccess

RewriteEngine on
```

```
RewriteCond  %{HTTPS} !=on
RewriteRule  ^/?(.*) https://%(SERVER_NAME)/$1 [R,L]
```

This should be added to the top before the AuthUserFile.

Once that is done, the next file that needs to be changed is the /etc/httpd/conf/httpd.conf file.

```
vi /etc/httpd/conf/httpd.conf
```

Add the file behind the AllowOveride AuthConfig setting

```
AllowOverride  AuthConfig  /var/www/html.htaccess
```

Restart using:

```
systemctl restart httpd
```

at this point an error came up and when the journal was looked at it said that there is an illegal override option of /var/www.html/.htacces. This shows that the file name was not typed in correctly so it was fixed and restart tried again. The same error showed up. As of yet, it is not working. Quotes were added and taken off and additional info typed into the file. It is not far off, though and should be working soon after more research on the topic and following the information in the journal -xe.

Conclusion.

The lab was mostly successful as the web server was set up with HTTPS, the certificates and the password protection. The student is confident that getting the HTTP to forward to HTTPS will work soon and when it does, the information will be added to the lab for personal use. Overall the student enjoyed the lab and hopes to make use of the knowledge by setting up a web server for the class project as well use at a future internship and career. Excellent lab.

References

Apache redirect to HTTPS. (2020). Namecheap.com Retrieved from https://www.namecheap.com/support/knowledgebase/article.aspx/9821/38/apache-redirect-to-https

Abrams, Lawrence. (November 29, 2019). *Kali Linux adds 'undercover' mode to impersonate* Windows 10. BleepingComputer. Retrieved from https://www.bleepingcomputer.com/news/security/kali-linux-adds-undercover-mode-to-impersonate-windows-10/

Bischoff, Paul. (March 28, 2019). *What is a NAT firewall and how does it work?* Comparitech. Retrieved from https://www.comparitech.com/blog/vpn-privacy/nat-firewall/

Brown, Korbin. (July3, 2017). *The beginners guide to iptables, the Linux firewall*. Retrieved from https://www.howtogeek.com/177621/the-beginners-guide-to-iptables-the-linux-firewall/

Centos Blog (2020). *What is Centos?* Retrieved from https://www.centosblog.com/what-is-centos/

Cheng, Simon M.C. (October 27, 2014). *Basic concept of ProxMox Virtual Environment.* Packt. Retrieved from https://hub.packtpub.com/basic-concepts-proxmox-virtual-environment/

Domantas, G. (March 25, 2020). What is Apache? An in-depth overview of Apache web server. Retrieved from https://www.hostinger.com/tutorials/what-is-apache

Ellingwood, Justin. (August 20, 2015). *How to forward ports through a Linux gateway with iptables.* Retrieved from https://www.digitalocean.com/community/tutorials/how-to-forward-ports-through-a-linux-gateway-with-iptables

Elwood. (November 26, 2019). *Kali Linux 2019.4 release*. Kali Linux News. Retrieved from https://www.kali.org/news/kali-linux-2019-4-release/

How to set up a firewall with FirewallD on CentOS7. (November 11, 2019). Linuxize. Retrieved from https://linuxize.com/post/how-to-setup-a-firewall-with-firewalld-on-centos-7/

Kenlon, Seth. (June24, 2019). Secure your Linux network with firewall-cmd. Retrieved from https://www.redhat.com/sysadmin/secure-linux-network-firewall-cmd

MDN contributors. (June 18, 2019). What is a web server? Retrieved from https://developer.mozilla.org/en-US/docs/Learn/Common_questions/What_is_a_web_server

ProxMox. (April 11, 2019). ProxMox.com Retrieved from https://www.proxmox.com/en/news/press-releases/proxmox-ve-5-4

RobetRSeattle. (March 13, 2017). *Start ssh automatically on boot.* AskUbuntu. Retrieved from https://askubuntu.com/questions/892447/start-ssh-automatically-on-boot

Singh, Shiv. (August 22, 2016). How to SSH on a port other than 22. Retrieved from https://askubuntu.com/questions/264046/how-to-ssh-on-a-port-other-than-22

SSH(Secure Shell). (2020). SSH.com. Retrieved from https://www.ssh.com/ssh

Vance, Nathan. (February 2, 2017). Understanding Firewalld in multi-zoned configurations. Retreieved from https://www.linuxjournal.com/content/understanding-firewalld-multi-zone-configurations

RobetRSeattle. (March 13, 2017). *Start ssh automatically on boot.* AskUbuntu. Retrieved from https://askubuntu.com/questions/892447/start-ssh-automatically-on-boot

Lab Network Topology

Kali2020VM--VMWare ethernet adapter--Student HP----(internal –router—external)

192.168.22.136 192.168.22.1 10.0.0.17 10.0.0.1 192.168.104.161

/

/

WWW

|

Gateway 10.42.0.1

|

chewy 10.42.0.31/16

|

darknet 172.16.0.3/16

|

External 172.16.242.32

router

Metasploitable VM 192.168.11.111 ----- Internal 192.168.11.1

/ \

Kali VM 192.168.11.10 WebServerVM 192.168.11.15