Lab 9- System Integrity

Dawn M Inman

CSC-432 Computer and Network Security

Professor Nick Merante

May 1, 2020

Abstract

This lab installs Tripwire on the CentOS 7 router VM. This is accomplished by updating CentOS 7, then installing Tripwire. The students email address is added to the configuration file so that email alerts can be sent when changes are made to the files. Encryption keys are added for system integrity. All of the files with Tripwire are encrypted for added security. An email is sent to the students file as a test and then changes are made to the files to see what alerts are set off on Tripwire and what it catches. Updating the configuration and data files for future monitoring were explored and cron was used to set up continuous monitoring which runs with a daily alert.

Keywords: Tripwire, encryption keys, integrity check, router VM, CentOS 7, Proxmox, KVM, QEMU.

Lab 9- System Integrity

System integrity means that a system is in the state of performing in an unimpaired manner. It implies that has not had any type of system manipulation, whether deliberate or accidental. Monitoring systems to make sure no unauthorized changes is a vital part of system administration for system integrity. This lab uses Tripwire as a tool for doing this monitoring. Tripwire is installed and set up for the best possible maintenance scenario with email alerts when changes happen.

This lab focuses on the router of the network. The router is facing the external traffic with the firewall in place and the virtual machines and Web Server VM behind the firewall and the router, creating an internal network. The virtual router being used is a CentOS 7 router which works with FirewallD. All of these are managed via Proxmox.

Tripwire is an open source software used for software security and data integrity. It can monitor file changes and give alerts when programmed for specific systems. It is a file integrity checker. Tripwire works by encrypting certain directories, files and information like checksums, file size, etc. It keeps these in a database that it compares with the monitored files and reports deviations to the administrator. The result is a system that has high integrity and can be relied upon to be unaltered. Tripwire was created in 1992 by Gene Kim and Dr. Eugene Spafford. Tripwire developed it further into Tripwire Enterprise. The open source project was begun in 2002 and is described as being suitable for small networks. (Benthin, 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)

FirewallD uses zones and services to manage and control the traffic that goes to and from the system (network). It manages by using trust levels for interfaces and network connections. The zones and services take the place of iptables that were previously used, making it more user friendly. These can be configured to create control to and from flow of traffic, whether it will be allowed or disallowed according to trust level, according to "How to set up a firewall with FirewallD on CentOS7". (November 11, 2019)

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)

Objective

This labs purpose is to create system integrity by installation and configuration of Tripwire, a file integrity checker. Keys are created for added security, email is added, configurations are changed, scans are run and an automatic scan job is created using cron.

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 console.

Results and Analysis[1]

Installation of Tripwire was straightforward. In the beginning the command line will be indented and the comments will be in parenthesis. The commands need to be run as the root user.

yum update -y (update CentOS 7, always a good idea to update)

yum install tripwire (installs tripwire)

(The configuration file needs to have the students email added. This is done by finding rule sets that appear important for notifications and then adding the email to each set. They look like:)

```
# File System and Disk Administration Programs
(
  rulename = “File system and Disk Administration Programs” ,
  severity   =  $(SIG_HI) ,
  emailto   =  dminman@utica.edu
)
```

(Encryption keys are made using:)

/usr/sbin/tripwire-setup-keyfiles

Files are encrypted for many reasons but one is to slow down potential attackers so they don't have easy access to files The second is to keep encrypted set as the back up for the plain text files when any files are left as plain text. This gives the opportunity for Tripwire to compare the two files to see if any differences are there, changes or modifications, and then send an alert if there are any.

(Then tripwire needs to be initialized:)

tripwire –init

(Analyze the filesystem with:)

tripwire –check –interactive

From here the report opens in vi and can be read. When it is closed the password key is prompted and once it is typed in the database file is written to /var/lib/tripwire/router-20200501-190845.twr. Each time a new change is made, a new database file is also made which changes the numbers at the end. The most recent file is at the bottom of the list when it is looked for. The following brings up the long list of database files:

ls -l /var/lib/tripwire/

To email the results of the interactive scan, type into the command line:

Tripwire –check –email-report

This sends the report to the email provided inside the configuration file. Here is the beginning of that file sent to the students' email.

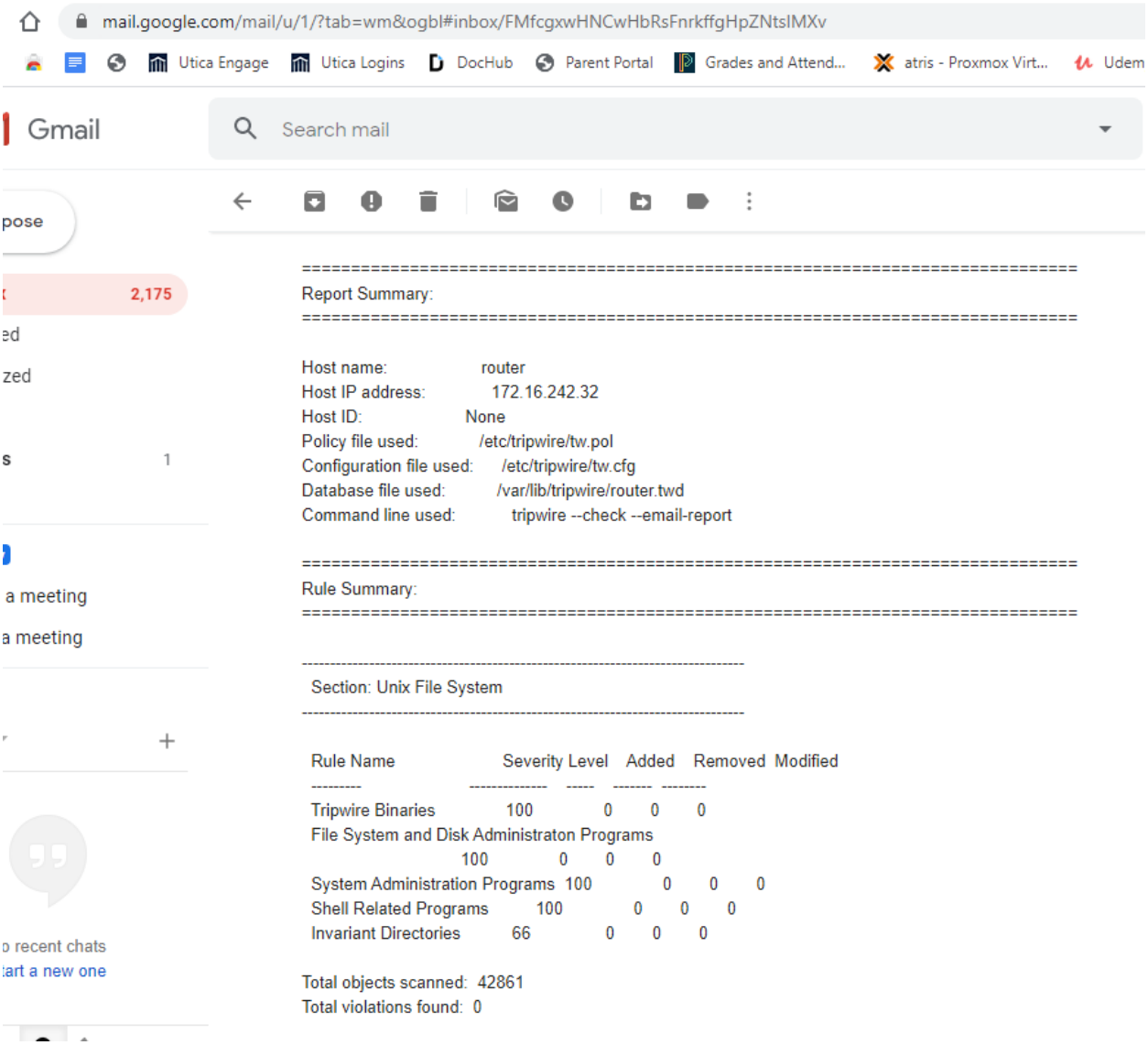


Figure 1 Tripwire report emailed to student

In the above picture there are zero violations found. The next objective is to play with some files to see if one or more violations can be made so that an alert is sent to the students email just by a violation happening. First the files in the config file are looked at so that the correct files can be modified to produce better results. This is done by typing in:

vi /etc/tripwire/twpol.txt

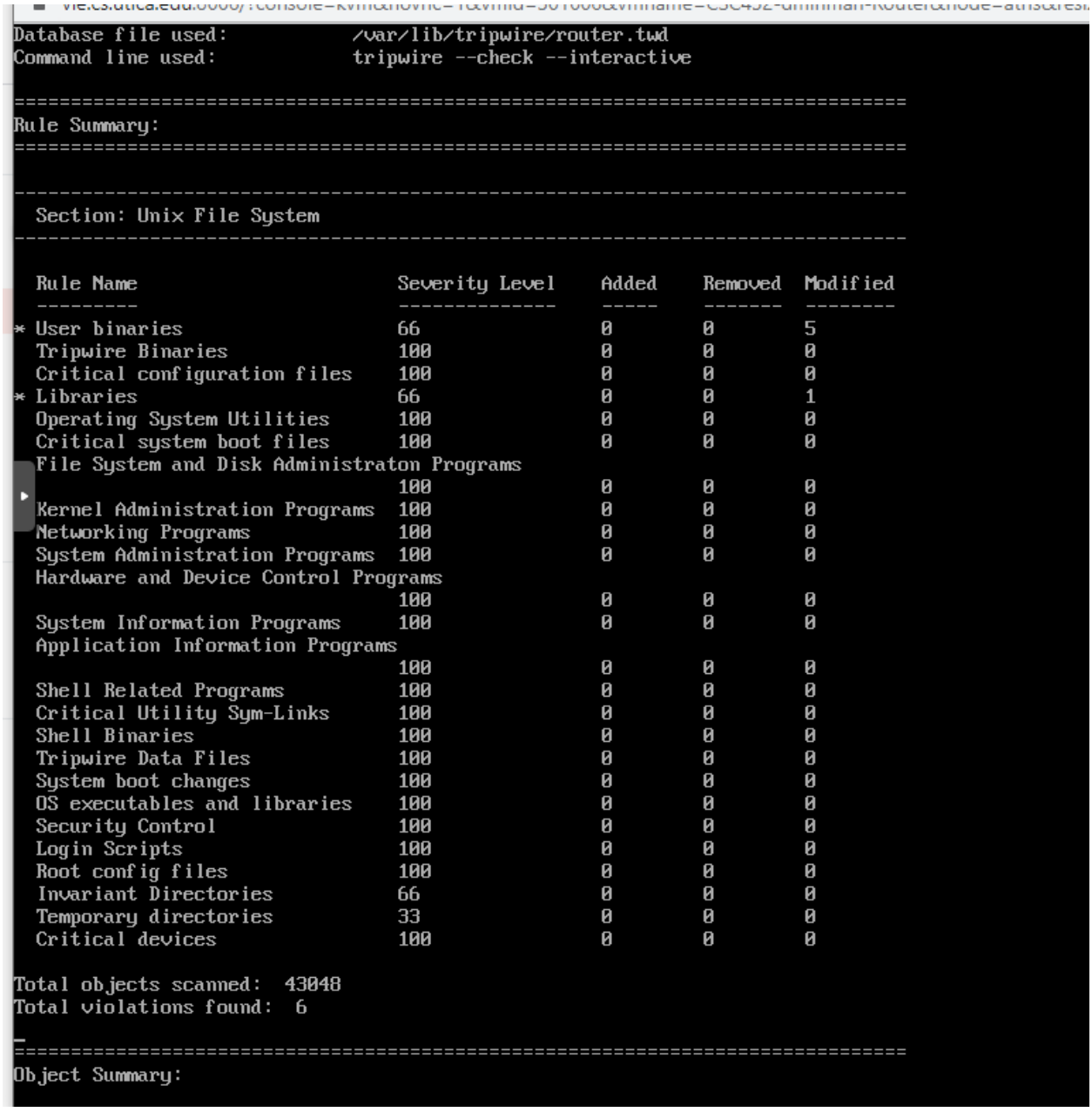
The files that are going to try being modified are /sbin/sshd-keygen, /bin/msginit, /sbin/newusers. They are modified at the beginning. All of these were encrypted files.

Now in root user, the report was run again.

Tripwire –check –email-report

Tripwire –check –interactive

The email report is listing the changes as 0, but the report that was run lists 6 violations on the first scan. After that, the scans say zero violations.



```
Database file used:           /var/lib/tripwire/router.twd
Command line used:            tripwire --check --interactive

===============================================================================
Rule Summary:
===============================================================================

-------------------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------------------

  Rule Name                     Severity Level    Added    Removed  Modified
  ---------                     --------------    -----    -------  --------
* User binaries                 66                0        0        5
  Tripwire Binaries             100               0        0        0
  Critical configuration files  100               0        0        0
* Libraries                     66                0        0        1
  Operating System Utilities    100               0        0        0
  Critical system boot files    100               0        0        0
  File System and Disk Administraton Programs
                                100               0        0        0
  Kernel Administration Programs 100              0        0        0
  Networking Programs           100               0        0        0
  System Administration Programs 100              0        0        0
  Hardware and Device Control Programs
                                100               0        0        0
  System Information Programs   100               0        0        0
  Application Information Programs
                                100               0        0        0
  Shell Related Programs        100               0        0        0
  Critical Utility Sym-Links    100               0        0        0
  Shell Binaries                100               0        0        0
  Tripwire Data Files           100               0        0        0
  System boot changes           100               0        0        0
  OS executables and libraries  100               0        0        0
  Security Control              100               0        0        0
  Login Scripts                 100               0        0        0
  Root config files             100               0        0        0
  Invariant Directories         66                0        0        0
  Temporary directories         33                0        0        0
  Critical devices              100               0        0        0

Total objects scanned:  43048
Total violations found:  6

===============================================================================
Object Summary:
```

In a production environment all files would need to be checked, but especially usernames, passwords, log in files and the like. Monitoring all files on a regular basis would be a necessity to make sure no malicious or inadvertent changes are being made to the system.

When changing the files to provide new checks, the database needs to be updated when the configuration file is updated. First a directory needs to be made of the missing files. This is done by typing:

sh -c “tripwire –check | grep Filename > missing-directory.txt

There is now a text file to refer to, so open the config file

/etc/tripwire/tw.cfg

To change the file put a # at the front of the line that needs to be taken out. For example, if the edit is /etc/rc.boot, then a # would go at the beginning of the line containing that file name. When finished, save and close the file. Regenerate the encrypted policy file:

twadmin -m P /etc/tripwire/twpol.txt

A password will be needed.

Now the database is reinitialized with:

Tripwire –init

Again, a password will be needed. When these are done, the database should be initialized without error. (Wallen, 2017)

To initialize a scan automatically, cron will be used to set it up. According to howtoforge, use the following to create a job for cron: first type on the command line, then type the second line into the file, save and exit

Crontab -e -u root

MAILTO=dminman@utica.edu

0 0 * * * /usr/sbin/tripwire –check –email-report

Save and exit.

The cron script will perform a tripwire system check daily. (Arul, 2020)

If more scans are wanted, the following produces a scan once per minute

* * * * *

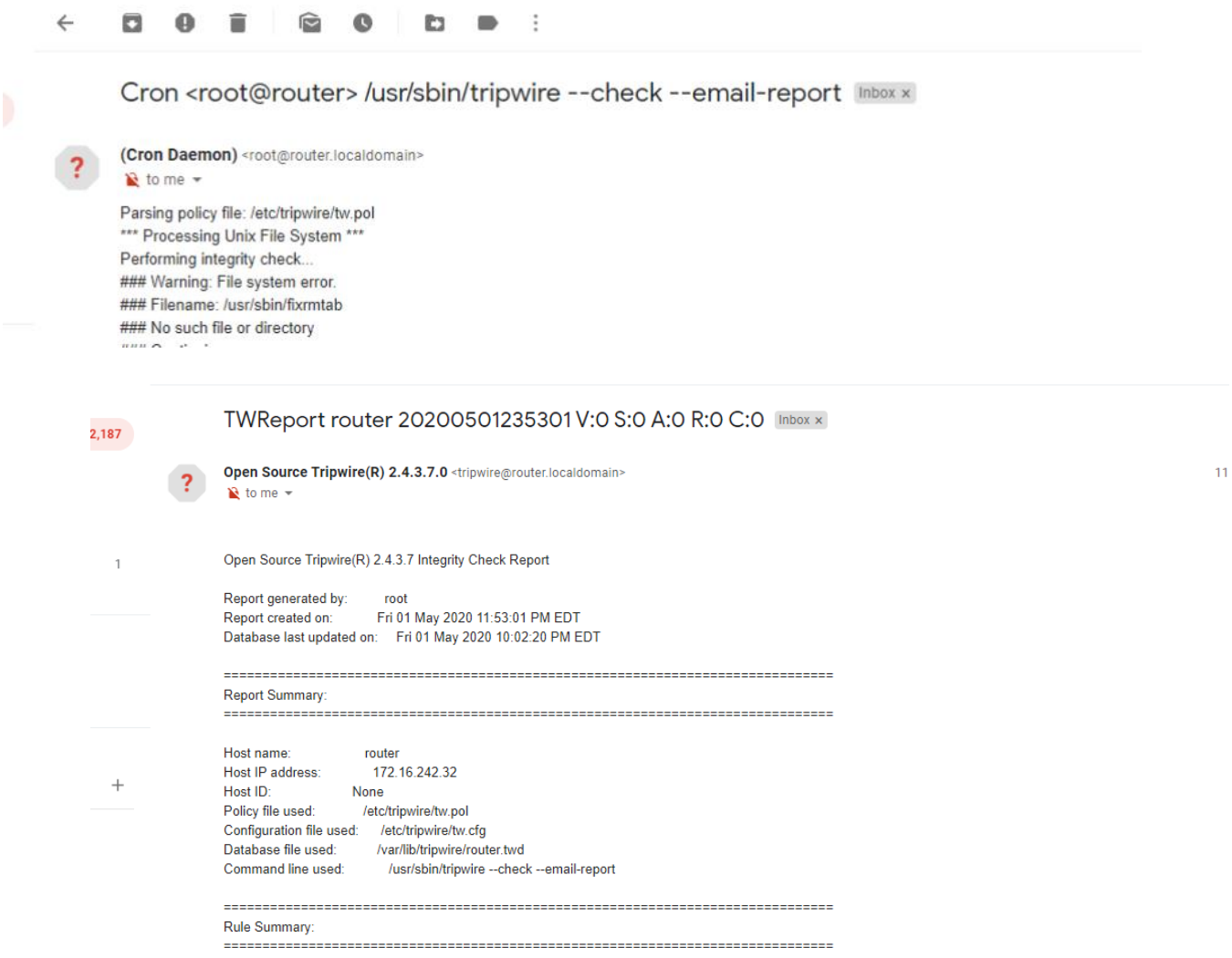
This scan will run every 5 minutes:

*/5 * * * *

This scan runs every hour:

0 * * * *

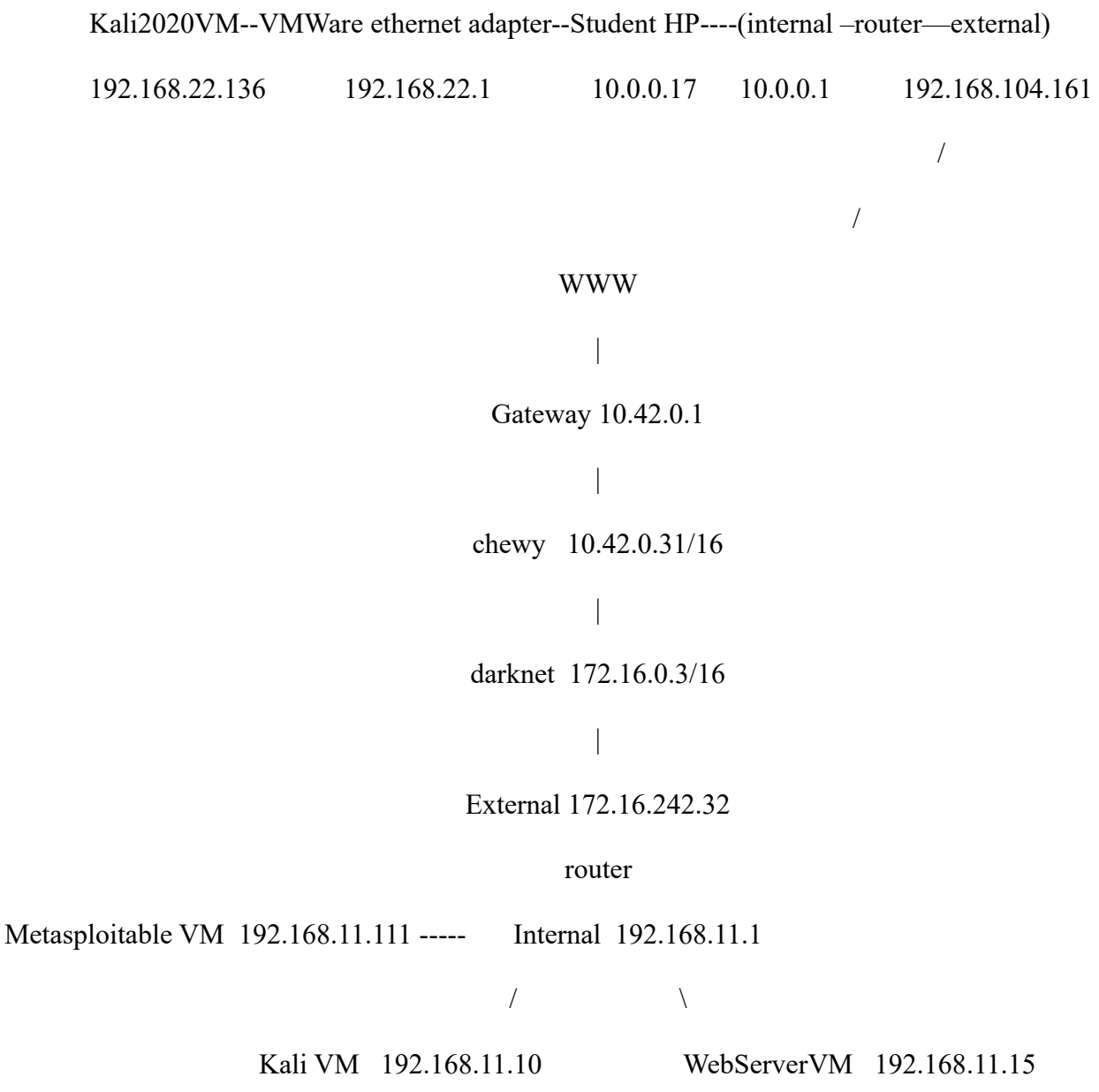
Whatever time is needed can be easily found at crontab guru. (Cronitor, 2020)



Conclusion.

This lab was successful in starting up Tripwire and performing system scans on the CentOS 7 VM. This lab was an excellent way to see how system administrators can keep track of even the smallest changes to a network and system. The downside of this type of system is that when the alert happens, an attack has already taken place and infiltrated the system. The benefits are that the system changes any attacker makes can be isolated and found quickly through the file system and the alerts that can be set up through email notifications. Turning off these notifications could be detrimental to an organization. Also, not configuring the alerts properly and testing them could produce issues. All areas of this would need to be tested to make sure Tripwire is working fully before relying on it is scan as a notice for intrusion. This was an excellent lab overall and will be useful in many different areas such as a senior project, computer science club and future employment.

Lab Network Topology



References

Arul, Muhammad. (2020). *Monitoring and detecting modified files using Tripwire on CenOS 7*. Retrieved from https://www.howtoforge.com/tutorial/monitoring-and-detecting-modified-files-using-tripwire-on-centos-7/

Benthin, Falko. (2020). *Detecting attackers with Tripwire.* Retrieved from https://www.linux-magazine.com/Online/Features/Detecting-Attackers-with-Tripwire

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/

Cronitor. (2020). Crontab guru. Retrieved from https://crontab.guru/every-1-hour

CSS (Computer Security Student). (2020). *Metasploitable project: lesson 2.* Retrieved from https://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/lesson2/index.html

Hoffman, Chris. (May 10, 2018). *How to upgrade to the latest version of ubuntu.* Retrieved from https://www.howtogeek.com/351360/how-to-upgrade-to-the-latest-version-of-ubuntu/

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/

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

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

Wallen, Jack. (November 1, 2017). *How to install and use Tripwire to detect modified files on Ubuntu server.* Retrieved from https://www.techrepublic.com/article/how-to-install-and-use-tripwire-to-detect-modified-files-on-ubuntu-server/

What is KVM? (2020) RedHat.com Retrieved from https://www.redhat.com/en/topics/virtualization/what-is-KVM