Lab #11: System Integrity

Franklin Nuth

CSC432 – Computer Information and Security

12 April 2019

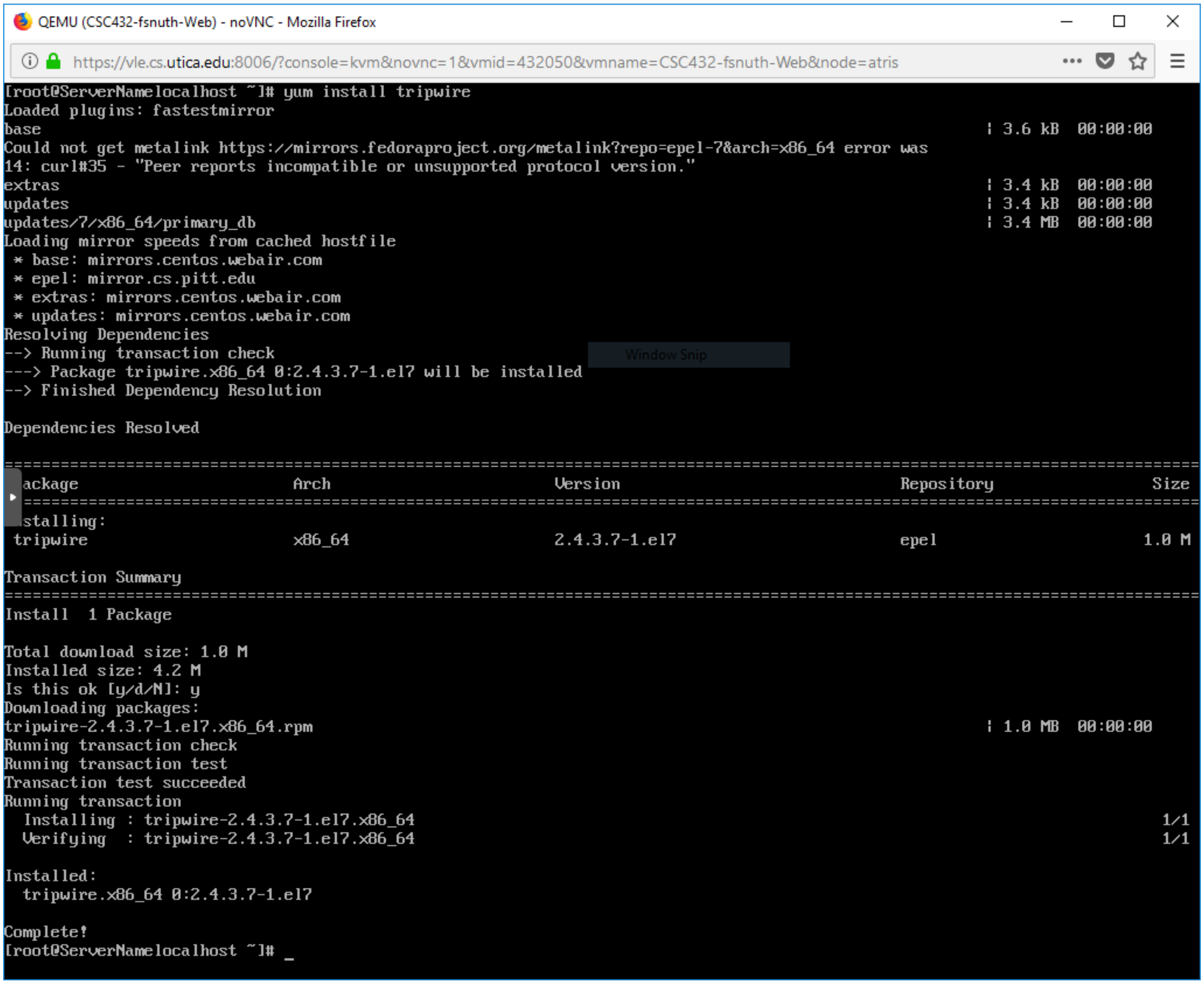
Abstract

The purpose of Lab 11 is to teach me how to maintain integrity on my network by using the appropriate software for the CentOS7 operating system. I will be installing a system integrity checker called Tripwire so that my web server will be equipped with the tools it needs to scan for modified or added files. I will also set it up in a way so that it can send a message to my college e-mail account whenever I do a manual scan. The software will also be configured in a way that it shall also automatically scan my web server's integrity at a set time daily.

Introduction

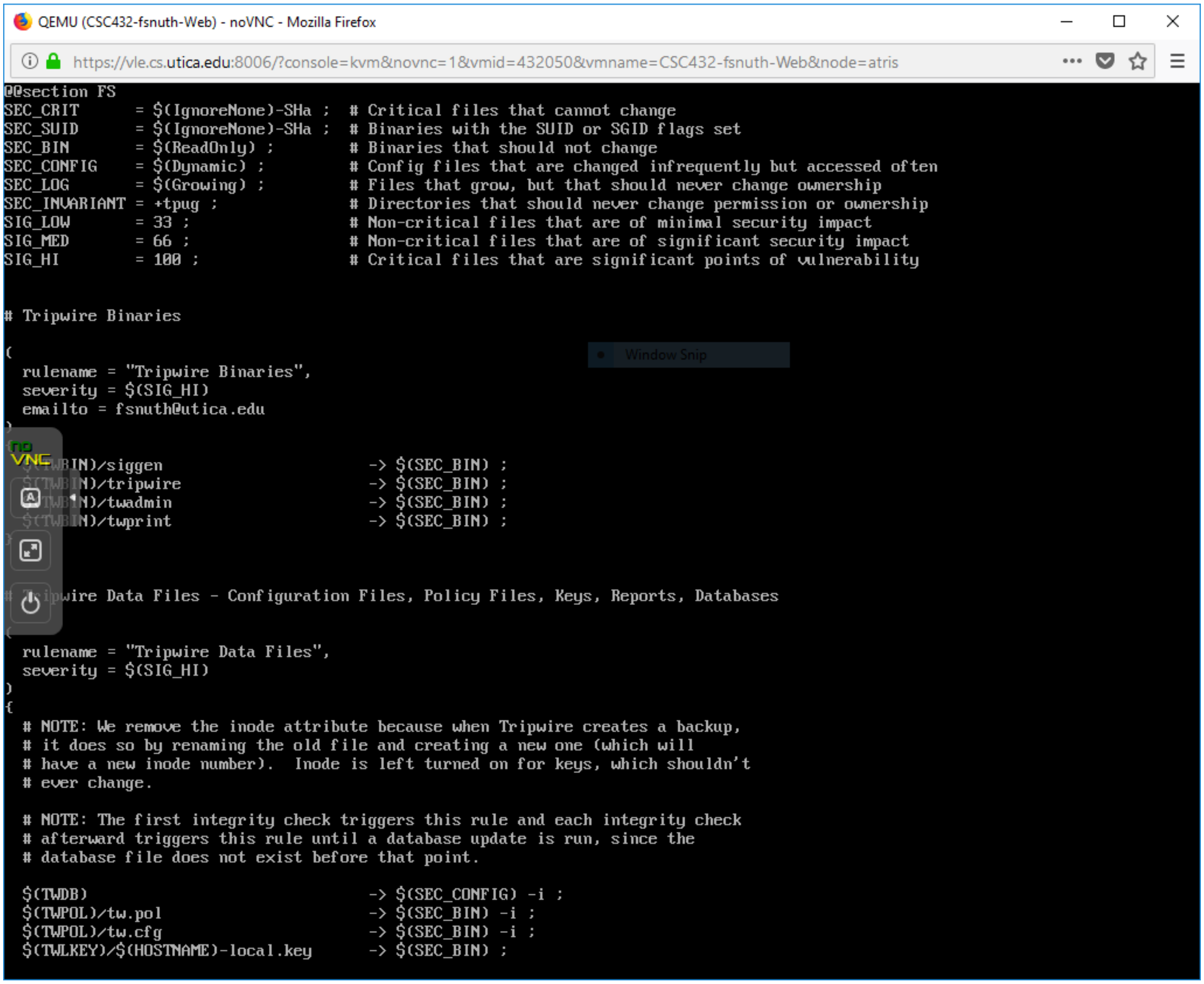
According to my information security class, the three principles of network security is confidentiality, accessibility, and integrity. All the labs I have done in the past are concerned with mostly the first two, since they dealt with minimizing vulnerabilities and making access more easier. In this lab, I will now work towards improving my network integrity by installing a software on my web server called Tripwire. By default, Tripwire is already set to help me out with system integrity when I scan manually on my web server. This lab will help me in automatic e-mail alerts whenever the integrity is compromised, and also help the web server scan itself with the Tripwire service automatically at whatever time I set it.

Processes & Screenshots


QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris
Window Snip

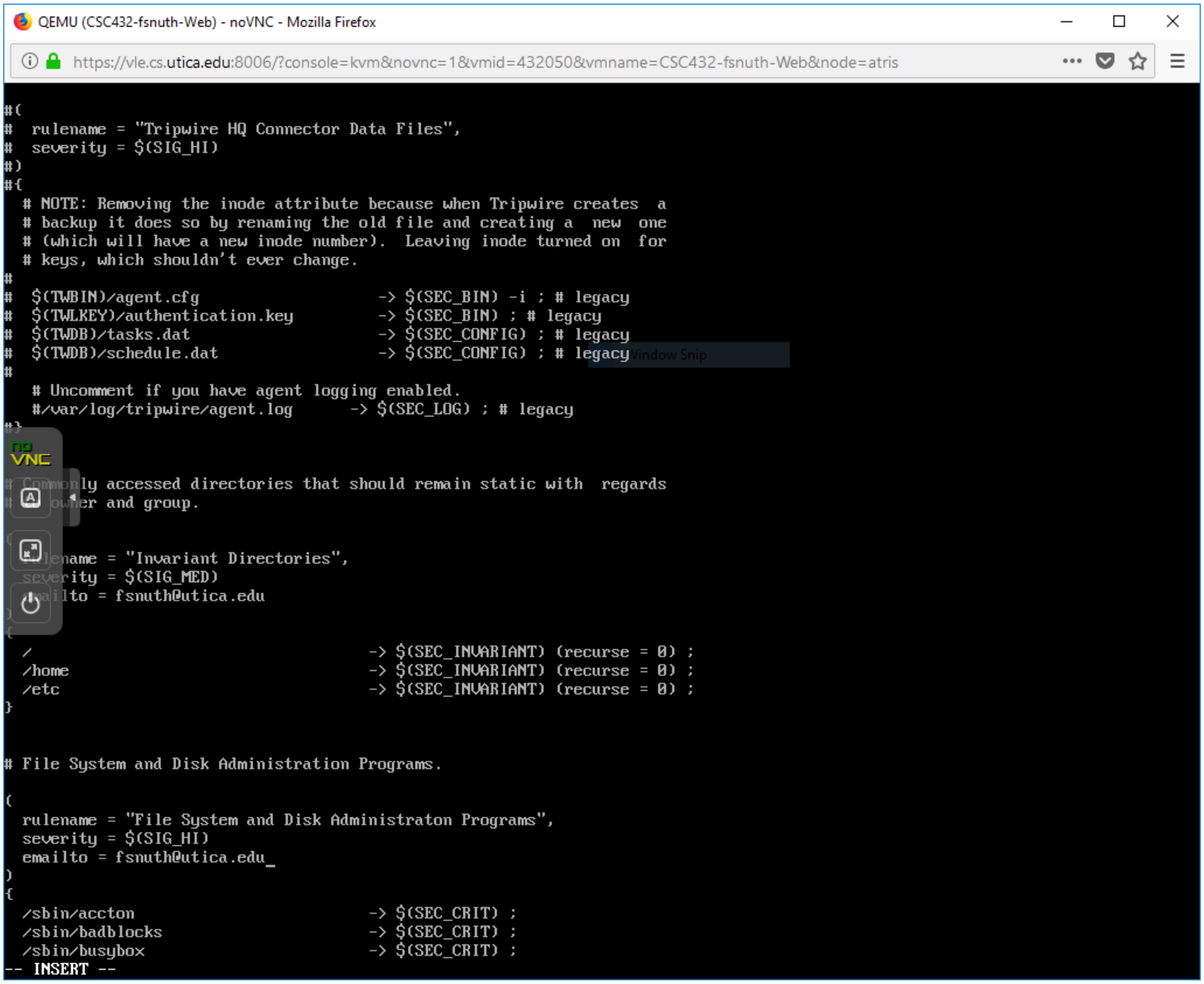
```
[root@ServerNamelocalhost ~]# yum install tripwire
Loaded plugins: fastestmirror
base                                                                                        | 3.6 kB  00:00:00
Could not get metalink https://mirrors.fedoraproject.org/metalink?repo=epel-7&arch=x86_64 error was
14: curl#35 - "Peer reports incompatible or unsupported protocol version."
extras                                                                                      | 3.4 kB  00:00:00
updates                                                                                     | 3.4 kB  00:00:00
updates/7/x86_64/primary_db                                                                 | 3.4 MB  00:00:00
Loading mirror speeds from cached hostfile
 * base: mirrors.centos.webair.com
 * epel: mirror.cs.pitt.edu
 * extras: mirrors.centos.webair.com
 * updates: mirrors.centos.webair.com
Resolving Dependencies
--> Running transaction check
---> Package tripwire.x86_64 0:2.4.3.7-1.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
  ackage                      Arch                     Version                           Repository           Size
================================================================================================================
  stalling:
 tripwire                     x86_64                   2.4.3.7-1.el7                     epel                1.0 M

Transaction Summary
================================================================================================================
Install  1 Package

Total download size: 1.0 M
Installed size: 4.2 M
Is this ok [y/d/N]: y
Downloading packages:
tripwire-2.4.3.7-1.el7.x86_64.rpm                                                           | 1.0 MB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : tripwire-2.4.3.7-1.el7.x86_64                                                                 1/1
  Verifying  : tripwire-2.4.3.7-1.el7.x86_64                                                                 1/1

Installed:
  tripwire.x86_64 0:2.4.3.7-1.el7

Complete!
[root@ServerNamelocalhost ~]# _
```

(The first thing we needed to do is install Tripwire along with all the dependencies it might need to run. We do that by going over to our web server and typing 'yum install tripwire'.)


QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris
noVNC
Window Snip

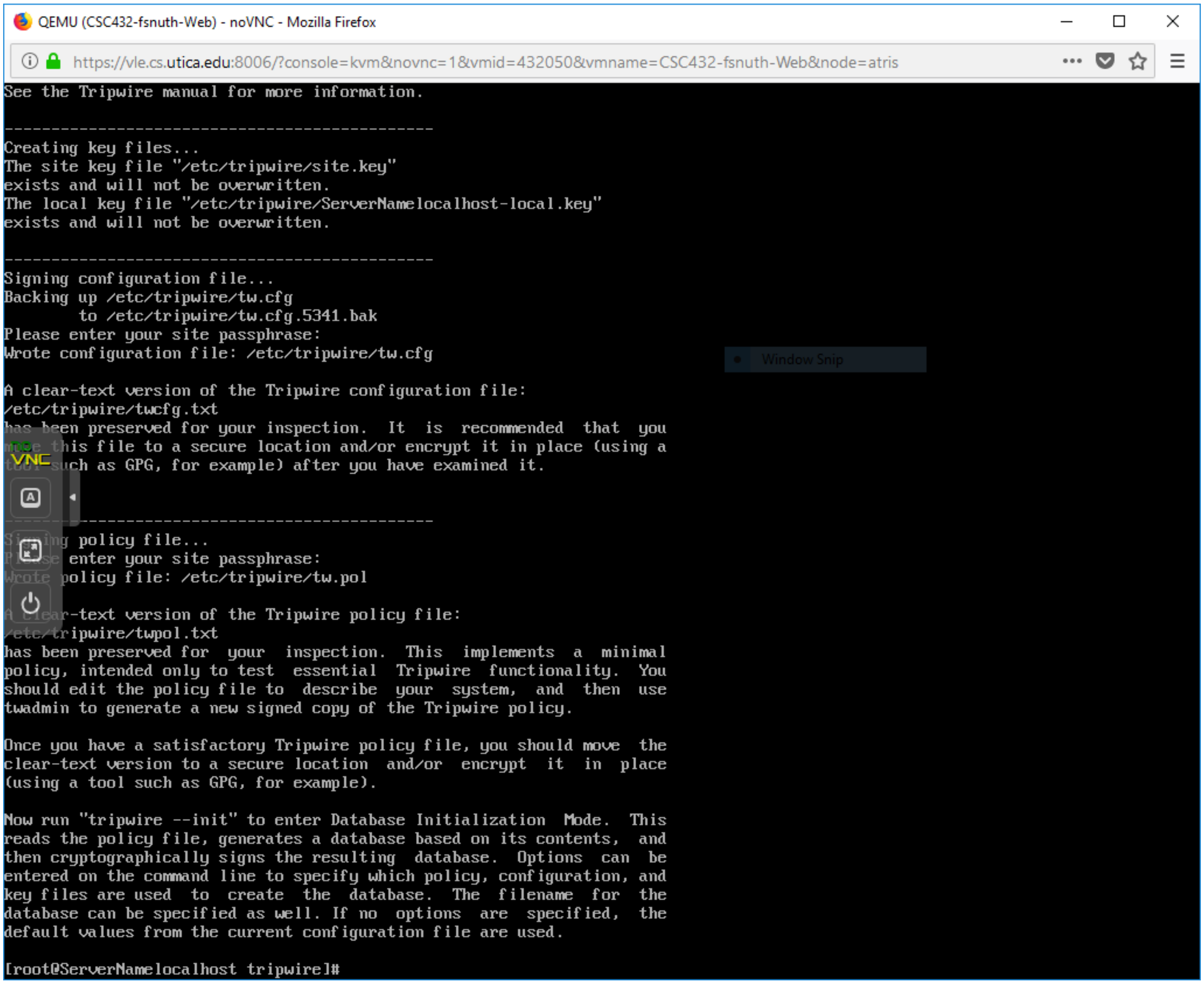
```
@@section FS
SEC_CRIT      = $(IgnoreNone)-SHa ;  # Critical files that cannot change
SEC_SUID      = $(IgnoreNone)-SHa ;  # Binaries with the SUID or SGID flags set
SEC_BIN       = $(ReadOnly) ;        # Binaries that should not change
SEC_CONFIG    = $(Dynamic) ;         # Config files that are changed infrequently but accessed often
SEC_LOG       = $(Growing) ;         # Files that grow, but that should never change ownership
SEC_INVARIANT = +tpug ;              # Directories that should never change permission or ownership
SIG_LOW       = 33 ;                 # Non-critical files that are of minimal security impact
SIG_MED       = 66 ;                 # Non-critical files that are of significant security impact
SIG_HI        = 100 ;                # Critical files that are significant points of vulnerability


# Tripwire Binaries

(
  rulename = "Tripwire Binaries",
  severity = $(SIG_HI)
  emailto = fsnuth@utica.edu
)
{
  $(TWBIN)/siggen                      -> $(SEC_BIN) ;
  $(TWBIN)/tripwire                    -> $(SEC_BIN) ;
  $(TWBIN)/twadmin                     -> $(SEC_BIN) ;
  $(TWBIN)/twprint                     -> $(SEC_BIN) ;
}


# Tripwire Data Files - Configuration Files, Policy Files, Keys, Reports, Databases

(
  rulename = "Tripwire Data Files",
  severity = $(SIG_HI)
)
{
  # NOTE: We remove the inode attribute because when Tripwire creates a backup,
  # it does so by renaming the old file and creating a new one (which will
  # have a new inode number).  Inode is left turned on for keys, which shouldn't
  # ever change.

  # NOTE: The first integrity check triggers this rule and each integrity check
  # afterward triggers this rule until a database update is run, since the
  # database file does not exist before that point.

  $(TWDB)                              -> $(SEC_CONFIG) -i ;
  $(TWPOL)/tw.pol                      -> $(SEC_BIN) -i ;
  $(TWPOL)/tw.cfg                      -> $(SEC_BIN) -i ;
  $(TWLKEY)/$(HOSTNAME)-local.key      -> $(SEC_BIN) ;
```

(After installing the Tripwire service and its dependencies, we go on to opening up the configuration file with 'vi /etc/tripwire/twpol.txt'. The 'twpol.txt' file is the policy file of my Tripwire service, and this is where we will soon set up some e-mailing features for our service. In the Tripwire Binaries section above, I entered a line called 'emailto = fsnuth@utica.edu'. This is the syntax that automatically sends fsnuth@utica.edu an emergency email for whenever something in my Tripwire directory has been changed or added.)


QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris
noVNC
Window Snip

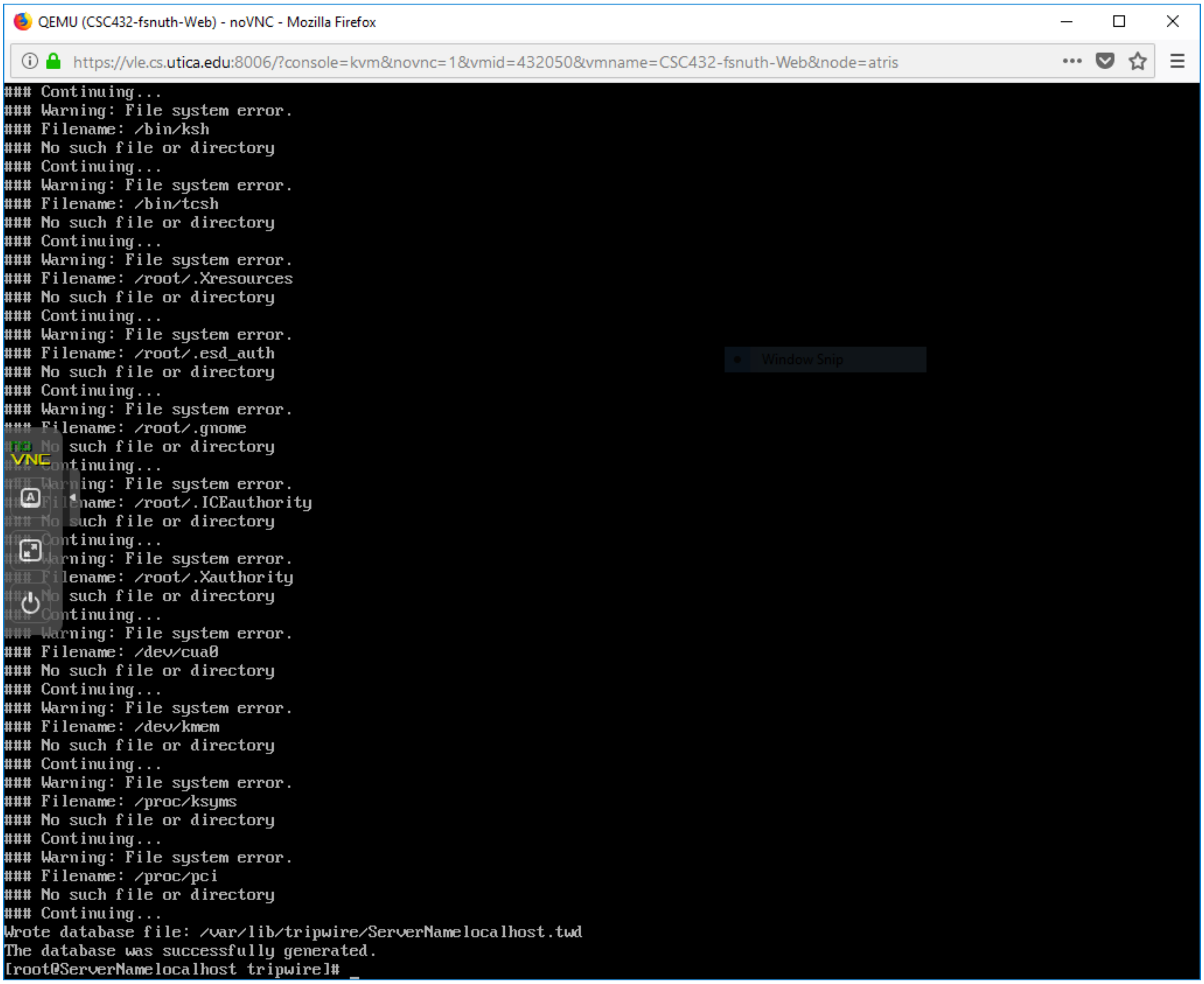
```
#(
#  rulename = "Tripwire HQ Connector Data Files",
#  severity = $(SIG_HI)
#)
#{
  # NOTE: Removing the inode attribute because when Tripwire creates  a
  # backup it does so by renaming the old file and creating a  new  one
  # (which will have a new inode number).  Leaving inode turned on  for
  # keys, which shouldn't ever change.
#
#  $(TWBIN)/agent.cfg                  -> $(SEC_BIN) -i ; # legacy
#  $(TWLKEY)/authentication.key        -> $(SEC_BIN) ; # legacy
#  $(TWDB)/tasks.dat                   -> $(SEC_CONFIG) ; # legacy
#  $(TWDB)/schedule.dat                -> $(SEC_CONFIG) ; # legacy
#
   # Uncomment if you have agent logging enabled.
   #/var/log/tripwire/agent.log      -> $(SEC_LOG) ; # legacy
#}


# Commonly accessed directories that should remain static with  regards
# to owner and group.

(
  rulename = "Invariant Directories",
  severity = $(SIG_MED)
  emailto = fsnuth@utica.edu
)
{
  /                                   -> $(SEC_INVARIANT) (recurse = 0) ;
  /home                               -> $(SEC_INVARIANT) (recurse = 0) ;
  /etc                                -> $(SEC_INVARIANT) (recurse = 0) ;
}


# File System and Disk Administration Programs.

(
  rulename = "File System and Disk Administraton Programs",
  severity = $(SIG_HI)
  emailto = fsnuth@utica.edu_
)
{
  /sbin/accton                        -> $(SEC_CRIT) ;
  /sbin/badblocks                     -> $(SEC_CRIT) ;
  /sbin/busybox                       -> $(SEC_CRIT) ;
-- INSERT --
```

(We scroll down for a bit for the sections 'Commonly accessed directories' and 'File Systems and Disk Administration Program'. We will do the same for what we did with Tripwire Binaries: we will set up alarms here with the same syntax as before. The only difference is that we now set up alarms for both our common directories and disk-related directories.)


QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris
VNC
Window Snip

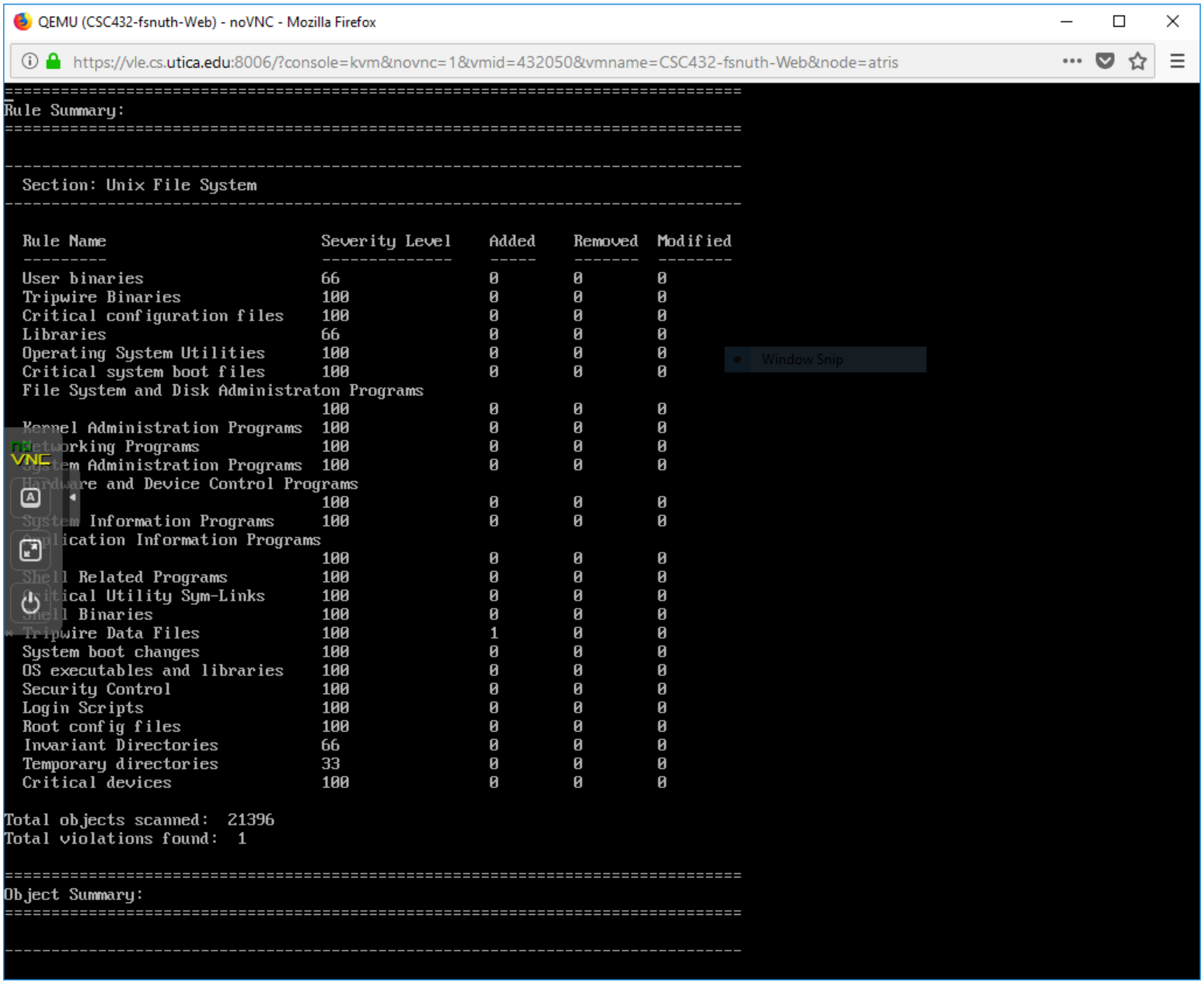
```
See the Tripwire manual for more information.

----------------------------------------------
Creating key files...
The site key file "/etc/tripwire/site.key"
exists and will not be overwritten.
The local key file "/etc/tripwire/ServerNamelocalhost-local.key"
exists and will not be overwritten.

----------------------------------------------
Signing configuration file...
Backing up /etc/tripwire/tw.cfg
        to /etc/tripwire/tw.cfg.5341.bak
Please enter your site passphrase:
Wrote configuration file: /etc/tripwire/tw.cfg

A clear-text version of the Tripwire configuration file:
/etc/tripwire/twcfg.txt
has been preserved for your inspection.  It  is  recommended  that  you
move this file to a secure location and/or encrypt it in place (using a
tool such as GPG, for example) after you have examined it.


----------------------------------------------
Signing policy file...
Please enter your site passphrase:
Wrote policy file: /etc/tripwire/tw.pol

A clear-text version of the Tripwire policy file:
/etc/tripwire/twpol.txt
has been preserved for  your  inspection.  This  implements  a  minimal
policy, intended only to test  essential  Tripwire  functionality.  You
should edit the policy file to  describe  your  system,  and  then  use
twadmin to generate a new signed copy of the Tripwire policy.

Once you have a satisfactory Tripwire policy file, you should move  the
clear-text version to a secure location  and/or  encrypt  it  in  place
(using a tool such as GPG, for example).

Now run "tripwire --init" to enter Database Initialization  Mode.  This
reads the policy file, generates a database based on its contents,  and
then cryptographically signs the resulting  database.  Options  can  be
entered on the command line to specify which policy, configuration, and
key files are used  to  create  the  database.  The  filename  for  the
database can be specified as well. If  no  options  are  specified,  the
default values from the current configuration file are used.

[root@ServerNamelocalhost tripwire]#
```

(After saving and writing the Tripwire policy file ('twpol.txt'), we then move on to generate encryption keys with '/usr/sbin/tripwire-setup-keyfiles'. I am then prompted to create my own site passphrase, which I should remember for later if I want to access anything Tripwire-related.)


QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris
noVNC
Window Snip

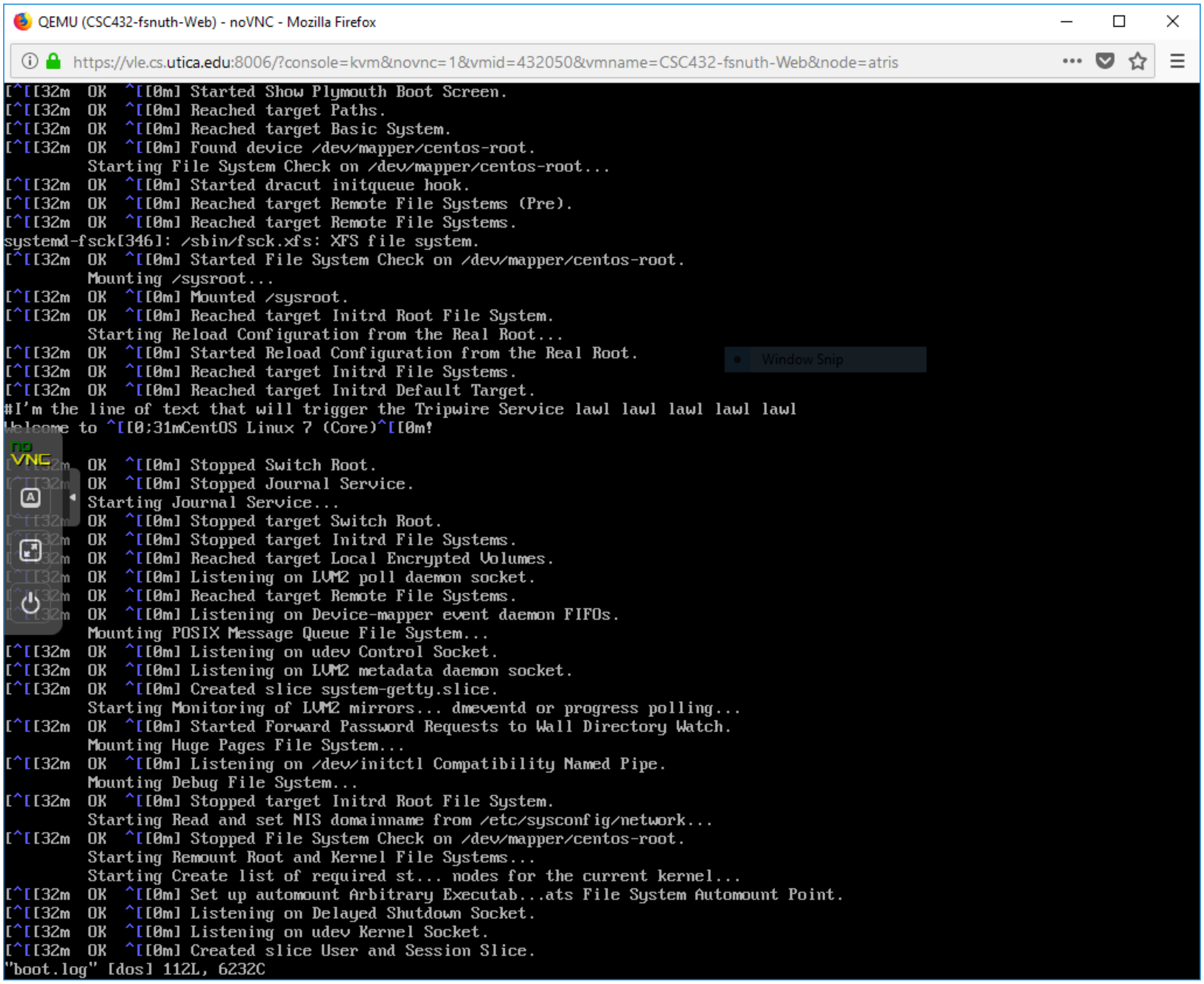
```
### Continuing...
### Warning: File system error.
### Filename: /bin/ksh
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /bin/tcsh
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.Xresources
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.esd_auth
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.gnome
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.ICEauthority
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /root/.Xauthority
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /dev/cua0
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /dev/kmem
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /proc/ksyms
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /proc/pci
### No such file or directory
### Continuing...
Wrote database file: /var/lib/tripwire/ServerNamelocalhost.twd
The database was successfully generated.
[root@ServerNamelocalhost tripwire]# _
```

(We then generate a new database with ‘tripwire –init’.)


QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris
noVNC
Window Snip

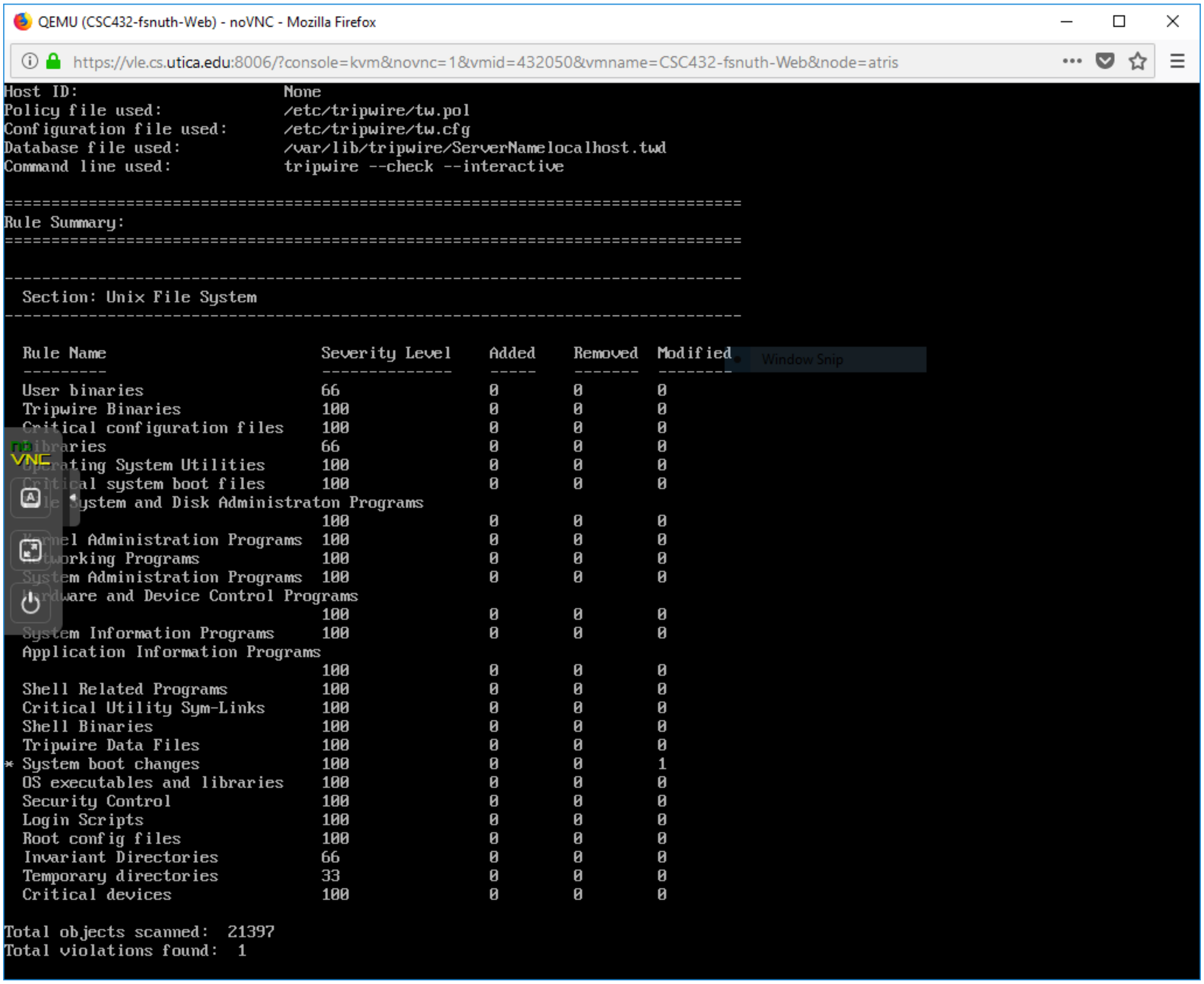
```
===============================================================================
Rule Summary:
===============================================================================

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

  Rule Name                       Severity Level    Added    Removed  Modified
  ---------                       --------------    -----    -------  --------
  User binaries                   66                0        0        0
  Tripwire Binaries               100               0        0        0
  Critical configuration files    100               0        0        0
  Libraries                       66                0        0        0
  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               1        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:  21396
Total violations found:  1

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

-------------------------------------------------------------------------------
```

(In order to manually generate a report with Tripwire, we use the syntax ‘tripwire - -check - -interactive’. This will pull up a report where anything in my web server has been changed or added.)


QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris
Window Snip
noVNC

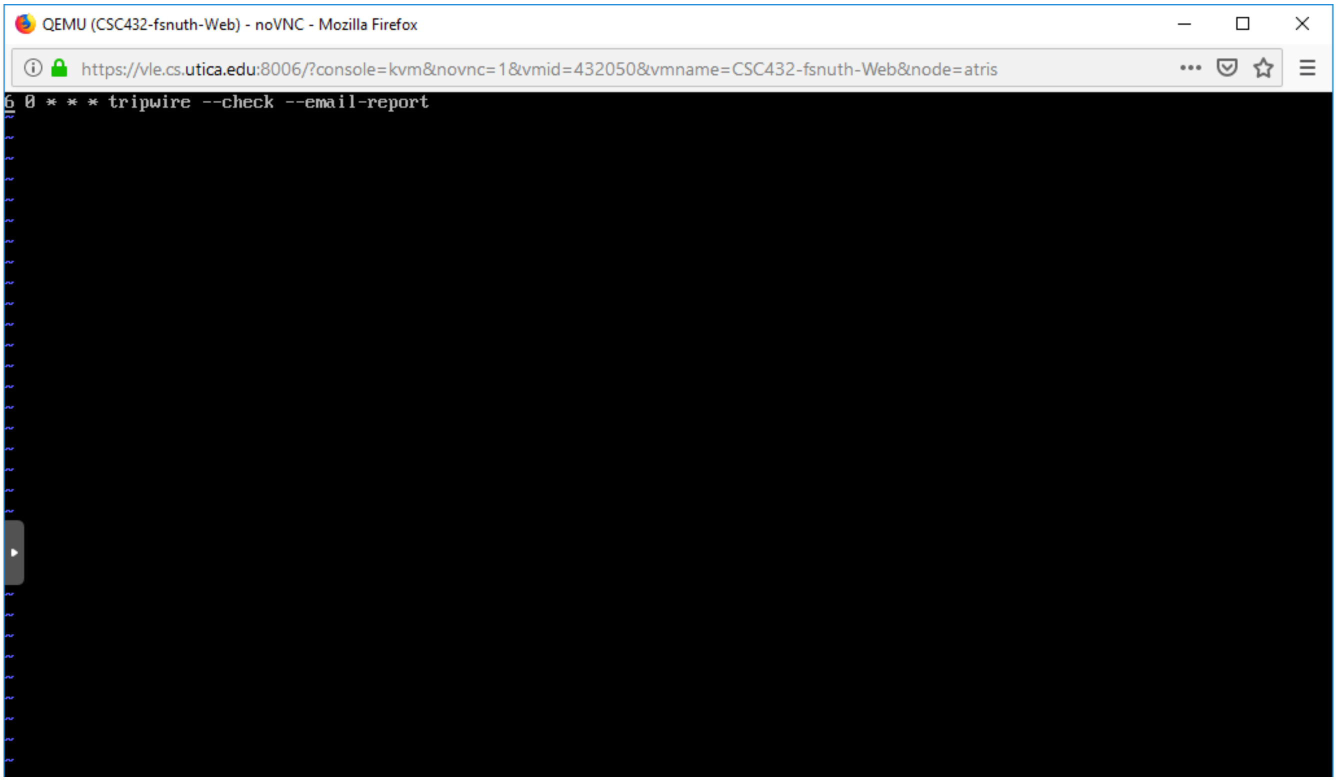
```
[^[[32m  OK  ^[[0m] Started Show Plymouth Boot Screen.
[^[[32m  OK  ^[[0m] Reached target Paths.
[^[[32m  OK  ^[[0m] Reached target Basic System.
[^[[32m  OK  ^[[0m] Found device /dev/mapper/centos-root.
         Starting File System Check on /dev/mapper/centos-root...
[^[[32m  OK  ^[[0m] Started dracut initqueue hook.
[^[[32m  OK  ^[[0m] Reached target Remote File Systems (Pre).
[^[[32m  OK  ^[[0m] Reached target Remote File Systems.
systemd-fsck[346]: /sbin/fsck.xfs: XFS file system.
[^[[32m  OK  ^[[0m] Started File System Check on /dev/mapper/centos-root.
         Mounting /sysroot...
[^[[32m  OK  ^[[0m] Mounted /sysroot.
[^[[32m  OK  ^[[0m] Reached target Initrd Root File System.
         Starting Reload Configuration from the Real Root...
[^[[32m  OK  ^[[0m] Started Reload Configuration from the Real Root.
[^[[32m  OK  ^[[0m] Reached target Initrd File Systems.
[^[[32m  OK  ^[[0m] Reached target Initrd Default Target.
#I'm the line of text that will trigger the Tripwire Service lawl lawl lawl lawl lawl
Welcome to ^[[0;31mCentOS Linux 7 (Core)^[[0m!

[^[[32m  OK  ^[[0m] Stopped Switch Root.
[^[[32m  OK  ^[[0m] Stopped Journal Service.
         Starting Journal Service...
[^[[32m  OK  ^[[0m] Stopped target Switch Root.
[^[[32m  OK  ^[[0m] Stopped target Initrd File Systems.
[^[[32m  OK  ^[[0m] Reached target Local Encrypted Volumes.
[^[[32m  OK  ^[[0m] Listening on LVM2 poll daemon socket.
[^[[32m  OK  ^[[0m] Reached target Remote File Systems.
[^[[32m  OK  ^[[0m] Listening on Device-mapper event daemon FIFOs.
         Mounting POSIX Message Queue File System...
[^[[32m  OK  ^[[0m] Listening on udev Control Socket.
[^[[32m  OK  ^[[0m] Listening on LVM2 metadata daemon socket.
[^[[32m  OK  ^[[0m] Created slice system-getty.slice.
         Starting Monitoring of LVM2 mirrors... dmeventd or progress polling...
[^[[32m  OK  ^[[0m] Started Forward Password Requests to Wall Directory Watch.
         Mounting Huge Pages File System...
[^[[32m  OK  ^[[0m] Listening on /dev/initctl Compatibility Named Pipe.
         Mounting Debug File System...
[^[[32m  OK  ^[[0m] Stopped target Initrd Root File System.
         Starting Read and set NIS domainname from /etc/sysconfig/network...
[^[[32m  OK  ^[[0m] Stopped File System Check on /dev/mapper/centos-root.
         Starting Remount Root and Kernel File Systems...
         Starting Create list of required st... nodes for the current kernel...
[^[[32m  OK  ^[[0m] Set up automount Arbitrary Executab...ats File System Automount Point.
[^[[32m  OK  ^[[0m] Listening on Delayed Shutdown Socket.
[^[[32m  OK  ^[[0m] Listening on udev Kernel Socket.
[^[[32m  OK  ^[[0m] Created slice User and Session Slice.
"boot.log" [dos] 112L, 6232C
```

(Because I set up an e-mail alarm in my File System and Disk Administration, it makes sense to add an obnoxious comment line or two in a file related to that area. The file that I chose for this one is 'boot.log', which is integral for my web server to boot up for use. Afterwards, I will check a manually generated report to see if Tripwire gets triggered.)


QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris
noVNC
Window Snip

```
Host ID:                       None
Policy file used:              /etc/tripwire/tw.pol
Configuration file used:       /etc/tripwire/tw.cfg
Database file used:            /var/lib/tripwire/ServerNamelocalhost.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        0
  Tripwire Binaries               100               0        0        0
  Critical configuration files    100               0        0        0
  Libraries                       66                0        0        0
  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        1
  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:  21397
Total violations found:  1
```

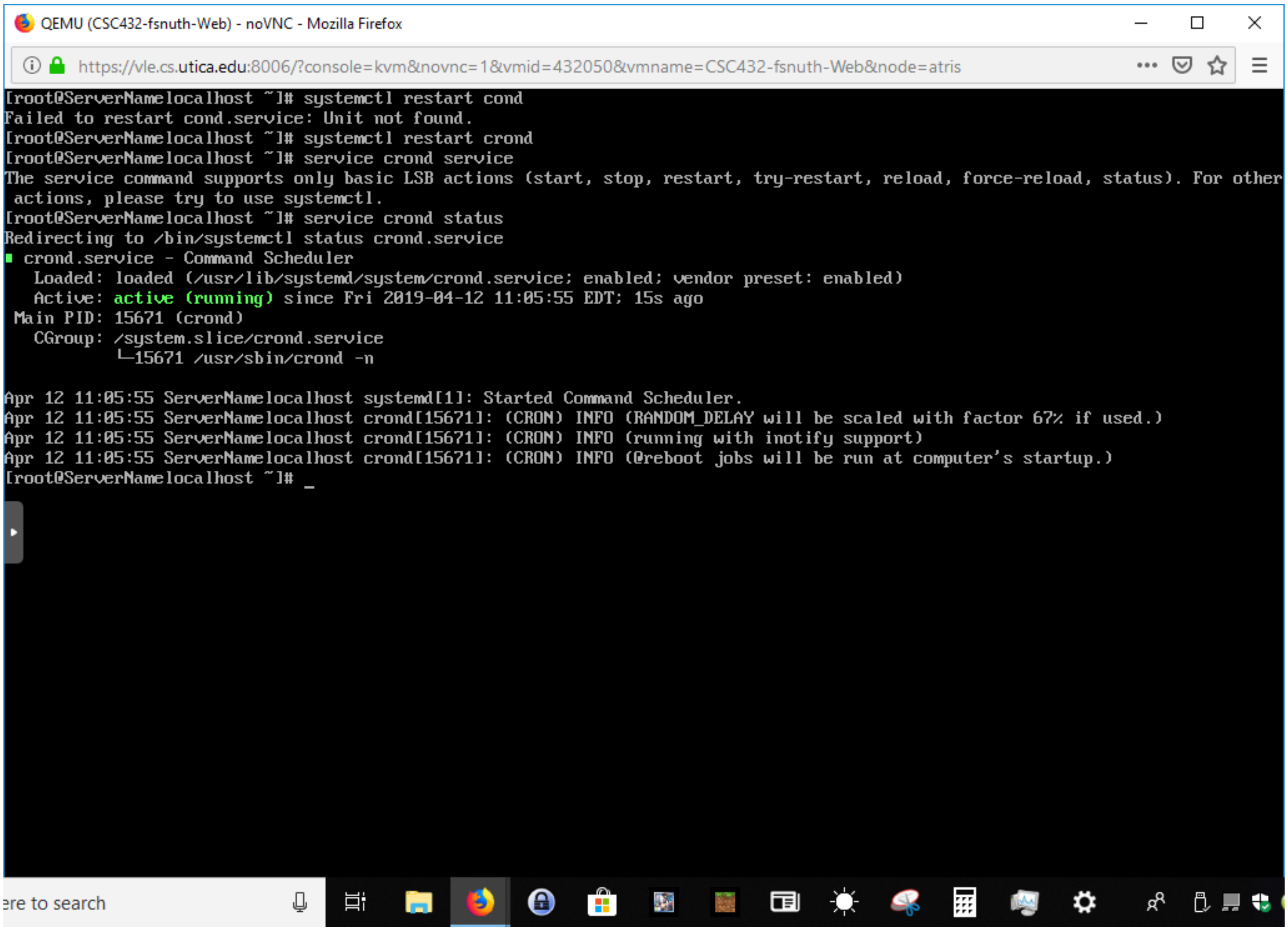
(I ended up learning that 'boot.log' is part of my System boot changes directory. Still, I achieved the feat of triggering the Tripwire system. I can imagine this being useful for serious administration work since Tripwire is even sensitive to new comments in the code, which often does no harm at all. In a productive environment, I would put a high value on all these rules by adding e-mail notifications to all of them. If I am an admin, I would want to know everything that is going on with all these rules.)



QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris

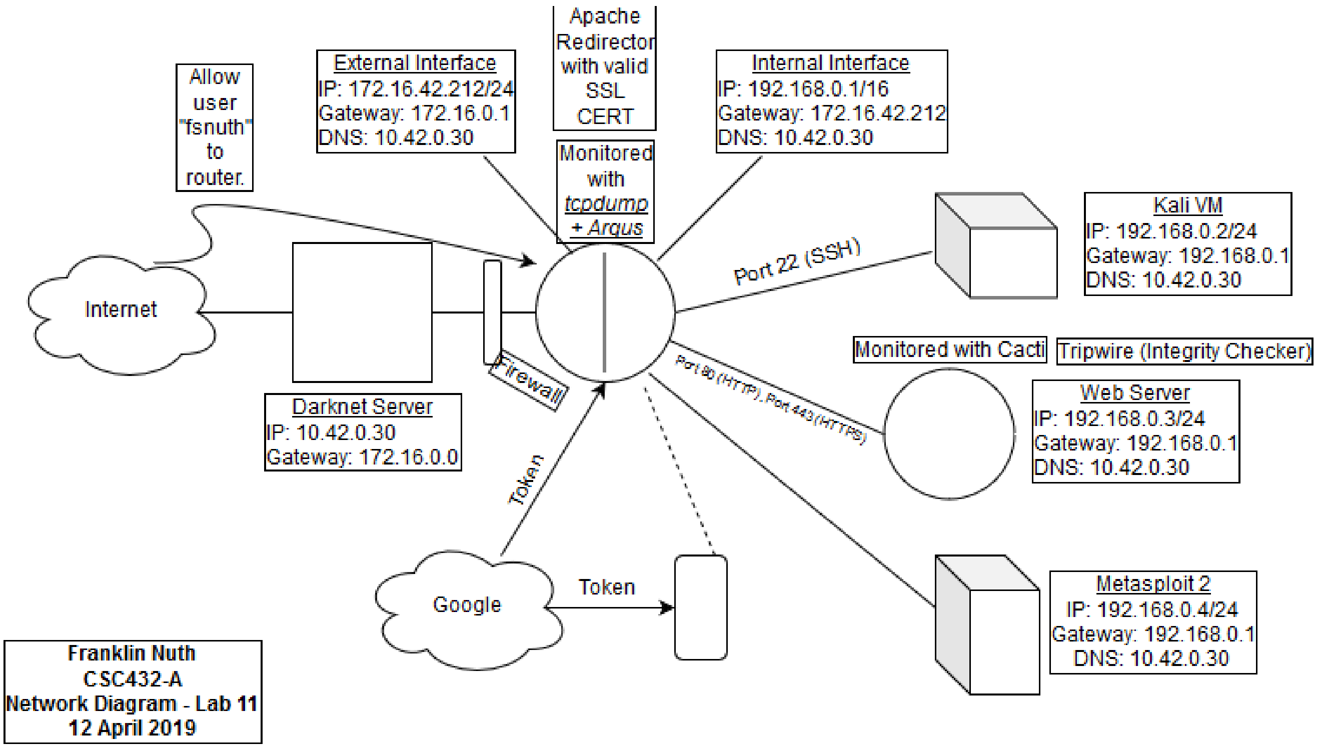
```
6 0 * * * tripwire --check --email-report
```

*(Setting up the 'cron' service to make an automatic e-mail feature with 'sudo crontab -e -u root'. This will open up an empty file that 'cron' will run. Above, my syntax is '6 0 * * * tripwire - -check - -email-report'. This means that every 6am, email me a Tripwire report.)*


QEMU (CSC432-fsnuth-Web) - noVNC - Mozilla Firefox
https://vle.cs.utica.edu:8006/?console=kvm&novnc=1&vmid=432050&vmname=CSC432-fsnuth-Web&node=atris
ere to search

```
[root@ServerNamelocalhost ~]# systemctl restart cond
Failed to restart cond.service: Unit not found.
[root@ServerNamelocalhost ~]# systemctl restart crond
[root@ServerNamelocalhost ~]# service crond service
The service command supports only basic LSB actions (start, stop, restart, try-restart, reload, force-reload, status). For other
 actions, please try to use systemctl.
[root@ServerNamelocalhost ~]# service crond status
Redirecting to /bin/systemctl status crond.service
● crond.service - Command Scheduler
   Loaded: loaded (/usr/lib/systemd/system/crond.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2019-04-12 11:05:55 EDT; 15s ago
 Main PID: 15671 (crond)
   CGroup: /system.slice/crond.service
           └─15671 /usr/sbin/crond -n

Apr 12 11:05:55 ServerNamelocalhost systemd[1]: Started Command Scheduler.
Apr 12 11:05:55 ServerNamelocalhost crond[15671]: (CRON) INFO (RANDOM_DELAY will be scaled with factor 67% if used.)
Apr 12 11:05:55 ServerNamelocalhost crond[15671]: (CRON) INFO (running with inotify support)
Apr 12 11:05:55 ServerNamelocalhost crond[15671]: (CRON) INFO (@reboot jobs will be run at computer's startup.)
[root@ServerNamelocalhost ~]# _
```

(Checking to make sure that my 'crond' is running with 'service crond status'. As indicated by the headings, 'crond' is good to go and running what I need it to run.)



(An updated version of my network diagram to represent my current topology at the time or writing this. My web server is fully equipped with the integrity checker 'Tripwire'.)

Issues & Resolutions

My issue with this lab is that my syntax for making adding the e-mail alerts to Tripwire's policy file was wrong. Originally, my syntax was 'emailto = fsnuth@utica.edu;'. This was only made apparent to me when I typed 'tripwire –test –email –fsnuth@utica.edu', and I did not get the usual test e-mail. I removed the semi-colon at the end, and made sure that my e-mail notifications are working again.

Conclusion

In this lab, I have set up Tripwire and modified it to my own needs as someone securing their network. I have configured the policy file with e-mail alerts so that I would be notified whenever anything in my network has been changed. I have also created encryption keys and generate databases so that Tripwire can begin doing its work. Now with automatic reporting to my e-mail account, my web server reports integrity to me like a weather forecaster. Unlike a weather forecast, it is up to me as a network administrator to utilize Tripwire to its fullest potential and make sure that everything in my network stays sunny.

References

die.net. 12 April 2019. *tripwire – Linux man page(8)*. Retrieved from: https://linux.die.net/man/8/tripwire

Hewlett Packard Enterprise Blog. 12 April 2019. *Tripwire Config Woes!* Retrieved from: https://community.hpe.com/t5/Security/TripWire-Config-Woes/td-p/3918580#.XK35ySApCM8

HowToForge Linux Tutorials. 12 April 2019. *Monitoring and Detecting Modified Files using Tripwire on CentOS 7.* Retrieved from: https://www.howtoforge.com/tutorial/monitoring-and-detecting-modified-files-using-tripwire-on-centos-7/

Kumar, Rahul. 24 November 2017. *Bash: mail: command not found (CentOS, Redhat, Ubuntu and Debian)*. Retrieved from: https://tecadmin.net/bash-mail-command-not-found/

Linux Questions.org. 12 April 2019. *tripwire not working (not sending e-mail)*. Retrieved from: https://www.linuxquestions.org/questions/linux-security-4/tripwire-not-working-not-sending-e-mail-186526/

Red Hat Linux 7.3: The Official Red Hat Linux Reference Guide. 12 April 2019. *Tripwire and Email*. Retrieved from: https://www-uxsup.csx.cam.ac.uk/pub/doc/redhat/redhat7.3/rhl-rg-en-7.3/s1-tripwire-email.html

Red Hat Linux 7.3: The Official Red Hat Linux Reference Guide. 12 April 2019. *Updating the Policy File*. Retrieved from: https://www-uxsup.csx.cam.ac.uk/pub/doc/redhat/redhat7.3/rhl-rg-en-7.3/s1-tripwire-update-policy.html