Host Data Integrity Baselining

The main aim of this lab is to create baselines of certain files within the Windows 7 operating system and Kali machine.

```
root@kali-lan: /etc
File  Edit  View  Search  Terminal  Help
root@kali-lan:~# pwd
/root
root@kali-lan:~# ls
Desktop
root@kali-lan:~# cd ..
root@kali-lan:/# ls
0     etc                 lib         media  root     srv  var
bin   example.conf.json   lib64       mnt    run      sys  vmlinuz
boot  home                live-build  opt    sbin     tmp
dev   initrd.img          lost+found  proc   selinux  usr
root@kali-lan:/# cd /etc
root@kali-lan:/etc# ls
adduser.conf          icedtea-web          postgresql
adjtime               iceweasel            postgresql-common
aliases               idmapd.conf          ppp
alternatives          ifplugd              profile
amap                  ImageMagick          profile.d
apache2               inetsim              protocols
apg.conf              init                 proxychains.conf
apm                   init.d               pulse
apt                   initramfs-tools      purple
arpwatch.conf         inittab              python
at.deny               inputrc              python2.6
at-spi2               insserv              python2.7
```

Figure 3.1

```
root@kali-lan: /etc
File  Edit  View  Search  Terminal  Help
gnome                 nikto.conf           unicornscan
gnome-vfs-2.0         nipper.conf          updatedb.conf
gnome-vfs-mime-magic  nsswitch.conf        UPower
groff                 ntp.conf             usb_modeswitch.conf
group                 obex-data-server     usb_modeswitch.d
group-                openal               vim
grub.d                openvas              vlc
gshadow               openvpn              vpnc
gshadow-              opt                  w3m
gssapi_mech.conf      os-release           wgetrc
gtk-2.0               PackageKit           wildmidi
gtk-3.0               pam.conf             wireshark
guymager              pam.d                wpa_supplicant
hal                   papersize            wvdial.conf
hdparm.conf           passwd               X11
host.conf             perl                 xdg
hostname              php5                 xml
hosts                 pkcs11               xpdf
hosts.allow           pm                   xprobe2
hosts.deny            polkit-1
root@kali-lan:/etc# md5sum passwd
6e6ea94fc3da6decf2e9cca2360569d6  passwd
root@kali-lan:/etc# md5sum passwd > ../root/Desktop/hashfile.md5
root@kali-lan:/etc#
```

Figure 3.2

On the kali linux machine, the cmd is opened and the **pwd** is used to determine your present working directory. The command **ls** is used to list the contents of the current

directory. Using the **cd/etc** command, we are navigating to the etc directory. As we see in figure 3.2, in the etc directory there is a file called passwd.

To display the MD5 hash of the passwd file, the following command is used: **md5sum passwd** and we can see the hash in the figure 3.2. To create a file for the hash, the following command is used: **md5sum passwd > ../root/Desktop/hashfile.md5**

```
Administrator: cmd - Shortcut
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>fciv
//
// File Checksum Integrity Verifier version 2.05.
//

Usage:  fciv.exe [Commands] <Options>

Commands: ( Default -add )

        -add    <file | dir> : Compute hash and send to output (default screen).

                dir options:
                -r        : recursive.
                -type     : ex: -type *.exe.
                -exc file: list of directories that should not be computed.
                -wp       : Without full path name. ( Default store full path)
                -bp       : specify base path to remove from full path name

        -list             : List entries in the database.
        -v                : Verify hashes.
                          : Option: -bp basepath.
```

Figure 3.3

Now, logging into the Windows 7 machine, the command **fciv** is used to show the options for the Microsoft File Checksum Integrity Verifier. It is used to create hashes or fingerprints of files within Windows.

```
Administrator: cmd - Shortcut
Options:
        -md5 | -sha1 | -both     : Specify hashtype, default md5.
        -xml db                  : Specify database format and name.

To display the MD5 hash of a file, type fciv.exe filename

C:\Windows\system32>cd c:\

c:\>fciv "c:\Program Files" -r -xml c_programfiles_baseline.xml
//
// File Checksum Integrity Verifier version 2.05.
//
Start Time: 10/20/2021 at 10h48'15''

Error loading XML document.
Create New XML database

End Time..: 10/20/2021 at 10h49'02''


        Processed 1711 directories
        Processed 11736 files
Errors have been reported to fciv.err

c:\>
```

Figure 3.4

To create a baseline of the program files directory on the C:\> drive and save the output to a file for validation, the following command is used:

fciv "c:\Program Files" -r -xml c_programfiles_baseline.xml

```
Administrator: cmd - Shortcut
        Processed 11736 files
Errors have been reported to fciv.err

c:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 68DC-CD09

 Directory of c:\

10/20/2021  10:39 AM             1,024 .rnd
10/20/2021  10:49 AM         1,843,005 c_programfiles_baseline.xml
10/20/2021  10:49 AM             7,309 fciv.err
05/28/2015  02:23 PM         1,568,438 graphviz.log
06/03/2015  06:23 PM    <DIR>          labfiles
07/13/2009  11:20 PM    <DIR>          PerfLogs
06/02/2015  09:22 AM    <DIR>          Program Files
06/02/2015  09:22 AM    <DIR>          Program Files (x86)
05/28/2015  02:23 PM           156,688 psqlodbc.log
06/01/2015  03:13 PM    <DIR>          Users
05/28/2015  02:23 PM         2,351,976 vcredist.log
06/02/2015  09:23 AM    <DIR>          Windows
               6 File(s)      5,928,440 bytes
               6 Dir(s)   8,319,131,648 bytes free

c:\>
```

Figure 3.5

After the baseline has been completed, the command **dir** is executed and as seen in figure 3.5, we can find the baseline xml file.

```
Administrator: cmd - Shortcut
c:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 68DC-CD09

 Directory of c:\

10/20/2021  10:39 AM             1,024 .rnd
10/20/2021  10:49 AM         1,843,005 c_programfiles_baseline.xml
10/20/2021  10:49 AM             7,309 fciv.err
05/28/2015  02:23 PM         1,568,438 graphviz.log
06/03/2015  06:23 PM    <DIR>          labfiles
07/13/2009  11:20 PM    <DIR>          PerfLogs
06/02/2015  09:22 AM    <DIR>          Program Files
06/02/2015  09:22 AM    <DIR>          Program Files (x86)
05/28/2015  02:23 PM           156,688 psqlodbc.log
06/01/2015  03:13 PM    <DIR>          Users
05/28/2015  02:23 PM         2,351,976 vcredist.log
06/02/2015  09:23 AM    <DIR>          Windows
               6 File(s)      5,928,440 bytes
               6 Dir(s)   8,319,131,648 bytes free

c:\>fciv -v -xml c_programfiles_baseline.xml > hashcheck.txt

c:\>_
```

Figure 3.6

We have to verify that no files have been changed, the **fciv** command is executed again to check the hashes that were computed and placed in baseline with the current files in the C:\ drive. The command used: **fciv -v -xml c_programfiles_baseline.xml > hashcheck.txt**

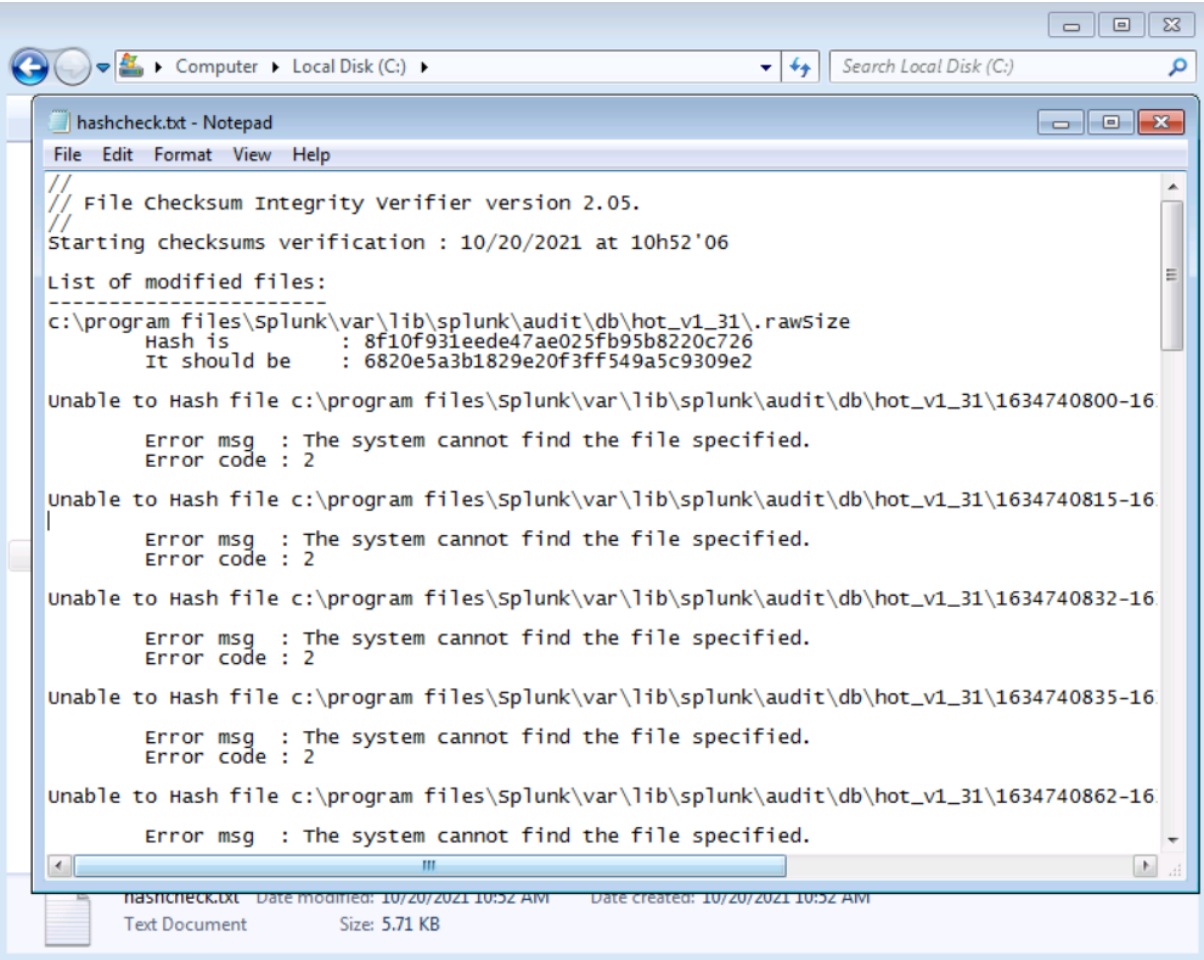

Figure 3.7

We see the output in the text file as redirected the standard output to a text file named “hashcheck.txt”.