

Name: Pankaj Parihar

Roll No.: 74

Batch: T21

Assignment – Hashdeep

Aim : To explore hashdeep tool in kali linux for generating, matching and auditing hash of files.

Theory :

Hashdeep on Ubuntu is utilized for file integrity verification and forensic analysis. Here's a theoretical overview of its purpose and functionality:

Overview of Hashdeep

1. Purpose:

- Hashdeep is designed to calculate and verify file hashes, ensuring data integrity and authenticity. It can help detect unauthorized changes to files, which is crucial for security audits and forensic investigations.

2. Supported Hash Algorithms:

- Hashdeep supports multiple hashing algorithms:
 - MD5
 - SHA-1
 - SHA-256
 - Tiger

3. Features:

- **Recursive Checking:** Hashdeep can scan directories and their subdirectories for file integrity checks.
- **Hash Comparisons:** It allows comparing computed hashes against known good hash values stored in a file.
- **Output Formats:** It can produce various output formats for logs and reports,

which is useful for record-keeping and analysis.

Use Cases

1. File Integrity Monitoring:

- Regularly compute and store hashes of important files to detect unauthorized modifications.

2. Forensic Investigations:

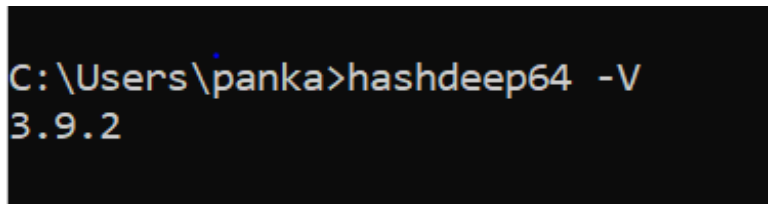
- Verify the integrity of digital evidence by comparing file hashes against known values.

3. Data Backup Verification:

- Ensure that backups have not been corrupted by comparing current file hashes against the original hashes.

Output:

1.



```
C:\Users\panka>hashdeep64 -V  
3.9.2
```

2.

```

C:\Users\panka>hashdeep64 -h
hashdeep64 version 3.9.2 by Jesse Kornblum.
C:\> hashdeep64 [-c <alg>] [-k <file>] [-amxwMXrespblvv] [-V|-h] [-o <mode>] [FILES]

-c <alg1,[alg2]> - Compute hashes only. Defaults are MD5 and SHA-256
    legal values are md5,sha1,sha256,tiger,whirlpool
-a - audit mode. Validates FILES against known hashes. Requires -k
-m - matching mode. Requires -k
-x - negative matching mode. Requires -k
-w - in -m mode, displays which known file was matched
-M and -X act like -m and -x, but display hashes of matching files
-k - add a file of known hashes
-r - recursive mode. All subdirectories are traversed
-e - compute estimated time remaining for each file
-s - silent mode. Suppress all error messages
-p - piecewise mode. Files are broken into blocks for hashing
-b - prints only the bare name of files; all path information is omitted
-l - print relative paths for filenames
-i - only process files smaller than the given threshold
-o - only process certain types of files. See README/manpage
-v - verbose mode. Use again to be more verbose.
-V - display version number and exit

C:\Users\panka>

```

3.

```

C:\Users\panka>hashdeep64 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: C:\Users\panka
## C:\> hashdeep64 1.txt
##
17,d7ad212c70a3554821e82463ef02aebc,87efedc1d68d10851dd38484f008288dc8da89b11da54fd7c8fc7c5002fffa,C:\Users\panka\1.txt

C:\Users\panka>

```

4.

```

C:\Users\panka>hashdeep64 -b 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: C:\Users\panka
## C:\> hashdeep64 -b 1.txt
##
17,d7ad212c70a3554821e82463ef02aebc,87efedc1d68d10851dd38484f008288dc8da89b11da54fd7c8fc7c5002fffa,1.txt

C:\Users\panka>

```

5.

```
C:\Users\panka>hashdeep64 -s 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: C:\Users\panka
## C:\> hashdeep64 -s 1.txt
##
17,d7ad212c70a3554821e82463ef02aebe,87efedc1d68d10851dd38484f008288dc8da89b11da54fdfd7c8fc7c5002fffa,C:\Users\panka\1.txt

C:\Users\panka>
```

6.

```
C:\Users\panka>hashdeep64 -c md5,sha1,sha256,tiger 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,sha256,tiger,filename
## Invoked from: C:\Users\panka
## C:\> hashdeep64 -c md5,sha1,sha256,tiger 1.txt
##
17,d7ad212c70a3554821e82463ef02aebe,b0615bb490f9d2d7a039e05772a7e40d7d5f1c3f,87efedc1d68d10851dd38484f008288dc8da89b11da54fdfd7c8fc7c5002fffa,f90c4c03122576e077e5cdef3ce65379fd47a1cf23ec54e7,C:\Users\panka\1.txt

C:\Users\panka>
```

7.

```
C:\Users\panka>hashdeep64 -c md5 *.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: C:\Users\panka
## C:\> hashdeep64 -c md5 *.txt
##
17,d7ad212c70a3554821e82463ef02aebe,C:\Users\panka\1.txt
7,6dafc65a085f7036aa526f29b8a48c2a,C:\Users\panka\abm.txt
786,fe12b44e7da8bc72529632c6597a4acd,C:\Users\panka\new 1.txt
0,d41d8cd98f00b204e9800998ecf8427e,C:\Users\panka\output.txt
2861,4b73b5218218451d2db4b1ae1bb1781a,C:\Users\panka\server.txt

C:\Users\panka>
```

8.

```

C:\Users\panka>hashdeep64 -c md5,sha1 *.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha1,filename
## Invoked from: C:\Users\panka
## C:\> hashdeep64 -c md5,sha1 *.txt
##
17,d7ad212c70a3554821e82463ef02aebe,b0615bb490f9d2d7a039e05772a7e40d7d5f1c3f,C:\Users\panka\1.txt
7,6dafc65a085f7036aa526f29b8a48c2a,7ad20906ed590bcd5acafe7e6b44e2d33ab1cc16,C:\Users\panka\abm.txt
786,fe12b44e7da8bc72529632c6597a4acd,383328e31e115d9c9ffe045aa7bbff88cca40fe6,C:\Users\panka\new 1.txt
0,d41d8cd98f00b204e9800998ecf8427e,da39a3ee5e6b4b0d3255bfe95601890afd80709,C:\Users\panka\output.txt
2861,4b73b5218218451d2db4b1ae1bb1781a,89f7789e1b3e08dad96411a68821a9b3f0273328,C:\Users\panka\server.txt

C:\Users\panka>

```

9.

```

C:\Users\panka>hashdeep64 -c md5 -p 100 1.txt
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: C:\Users\panka
## C:\> hashdeep64 -c md5 -p 100 1.txt
##
17,d7ad212c70a3554821e82463ef02aebe,C:\Users\panka\1.txt offset 0-16

C:\Users\panka>

```

10.

```

C:\Users\panka>mkdir Pankaj

C:\Users\panka>cd Pankaj

C:\Users\panka\Pankaj>hashdeep64 -c md5 .
C:\Users\panka\Pankaj: Is a directory

```

11.

```
C:\Users\panka\Pankaj>md5deep *.txt > newFile.txt
md5deep: WARNING: You are running a 32-bit program on a 64-bit system.
md5deep: You probably want to use the 64-bit version of this program.

C:\Users\panka\Pankaj>md5deep64 *.txt > newFile.txt

C:\Users\panka\Pankaj>cat newFile.txt
'cat' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\panka\Pankaj>type newFile.txt
d41d8cd98f00b204e9800998ecf8427e C:\Users\panka\Pankaj\newFile.txt

C:\Users\panka\Pankaj>hashdeep64 *.txt > newFile2.txt

C:\Users\panka\Pankaj>type newFile2.txt
%%%% HASHDEEP-1.0
%%%% size,md5,sha256,filename
## Invoked from: C:\Users\panka\Pankaj
## C:\> hashdeep64 *.txt
##
69,e2295b28ae0f852c520282bb4f0feda5,88e404ce262211cf189db7e655c1bb833d0b3619401f61a7dd73525087440213,C:\Users\panka\Pankaj\newFile.txt
0,d41d8cd98f00b204e9800998ecf8427e,e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855,C:\Users\panka\Pankaj\newFile2.txt

C:\Users\panka\Pankaj>
```

12.

```
C:\Users\panka\Pankaj>hashdeep64 -c md5 -r .
%%%% HASHDEEP-1.0
%%%% size,md5,filename
## Invoked from: C:\Users\panka\Pankaj
## C:\> hashdeep64 -c md5 -r .
##
69,e2295b28ae0f852c520282bb4f0feda5,C:\Users\panka\Pankaj\newFile.txt
393,d8a0253f58d78f2cc25e667e0bb14555,C:\Users\panka\Pankaj\newFile2.txt

C:\Users\panka\Pankaj>
```

Conclusion: Demonstrated key management, distribution and user authentication (LO2 is achieved).