Linux Assignment 2

Name:Murungi Happy

ID:27654

1.

• **System configuration files an attacker might modify: /etc** (primary), also **/boot**, **/home** (user configs), **/opt** (third-party app configs).

• **Essential binaries that could be replaced with malicious ones: /bin** and **/usr** (especially `/usr/bin`, `/usr/sbin`), also `/opt` and sometimes `/sbin` or `/usr/local/bin`.

• **Log files that might show intrusion evidence: /var** (especially `/var/log`), also user histories under **/home** and system journals in `/run` or `/var/run` (and `journalctl`).

/bin

- **What it contains:** Essential user commands required at boot and single-user mode (`ls`, `cp`, `sh`, etc.).
- **Why attacker cares:** Replacing `/bin` binaries lets an attacker persist or hide activity (backdoored `ls`, `ps`, `sh`).
- **Category: Essential binaries** (high risk).

/etc

- **What it contains:** System configuration files (network, services, users, auth, startup scripts): e.g. `passwd`, `shadow`, `ssh/sshd_config`, `fstab`, `crontab` entries, service configs.
- **Why attacker cares:** Changing configs can create backdoors (enable root login, add SSH keys, alter sudoers), create persistence, change auditing.
- **Category: System configuration files** (primary target).

/var

- **What it contains:** Variable data: logs (`/var/log`), spools, mail, caches, databases.

- **Why attacker cares:** Logs show intrusion evidence (auth failures, sudo uses, service restarts). Attackers may also delete/modify logs or write to `/var/tmp`.
- **Category: Log files / evidence** (primary), also useful for temporary/persistent data.

/usr

- **What it contains:** Secondary hierarchy for user utilities and applications — `/usr/bin`, `/usr/sbin`, `/usr/lib`.
- **Why attacker cares:** Many production binaries live here; attackers may replace `/usr/bin` tools or add malicious versions. `/usr/local` is often writable for local installs and abused.
- **Category: Essential binaries** (high risk).

/tmp

- **What it contains:** World-writable temporary files. Typically cleared periodically.
- **Why attacker cares:** Easy place to drop tools, store payloads, or use for socket/listener. Setuid/cron abuse sometimes uses `/tmp`. Also a common staging area for privilege escalation.
- **Category: Staging / temporary malicious files** (check for malware but not primary config/binaries).

/opt

- **What it contains:** Optional third-party or add-on application software and their configs.
- **Why attacker cares:** Third-party apps may be replaced or backdoored here (especially if vendor packages are installed here). Attackers may install tools in `/opt` for persistence.
- **Category: Third-party binaries & configs** (could be either binaries or configs).

/boot

- **What it contains:** Kernel images, initramfs, bootloader config (e.g., GRUB).
- **Why attacker cares:** Modifying kernel/initrd or bootloader can give persistent, stealthy control (boot-time rootkits). Changes here are high-impact but require privileges.
- **Category: System configuration / boot binaries** (important for rootkit/persistence detection).

/home

- **What it contains:** User home directories, dotfiles (`.bashrc`, `.ssh/authorized_keys`), user data and histories.
- **Why attacker cares:** Place to hide backdoors, add SSH keys, modify user profiles to escalate. User shell histories (`.bash_history`), `.ssh/` and hidden files often contain traces or indicators. Compromised user accounts yield lateral movement.
- **Category: User configs & evidence** (also staging for persistence).

Investigation

2.

```
mkdir -p ~/projects/client_work/web/{frontend,backend,database} \
~/projects/client_work/mobile/{ios,android} \
~/projects/personal/{experiments,archive} \
~/projects/shared/{templates,resources}
```

- `mkdir -p`: Creates directories and their parent directories as needed.
- `~/projects/`: The base directory where all projects will be created.
- The curly braces `{}` are used to create multiple directories at once.

3.

pwd

cd ../../../personal/experiments

pwd

cd ../../shared/templates

pwd

cd ../../../client_work/web/frontend

pwd

```
HP@Happy MINGW64 ~/projects
$ pwd
/c/Users/HP/projects

HP@Happy MINGW64 ~/projects
$ cd personal/experiments

HP@Happy MINGW64 ~/projects/personal/experiments
$ pwd
/c/Users/HP/projects/personal/experiments

HP@Happy MINGW64 ~/projects/personal/experiments
$ cd ../../shared/templates

HP@Happy MINGW64 ~/projects/shared/templates
$ pwd
/c/Users/HP/projects/shared/templates

HP@Happy MINGW64 ~/projects/shared/templates
$ cd ../../client_work/web/frontend

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ pwd
/c/Users/HP/projects/client_work/web/frontend

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$
```

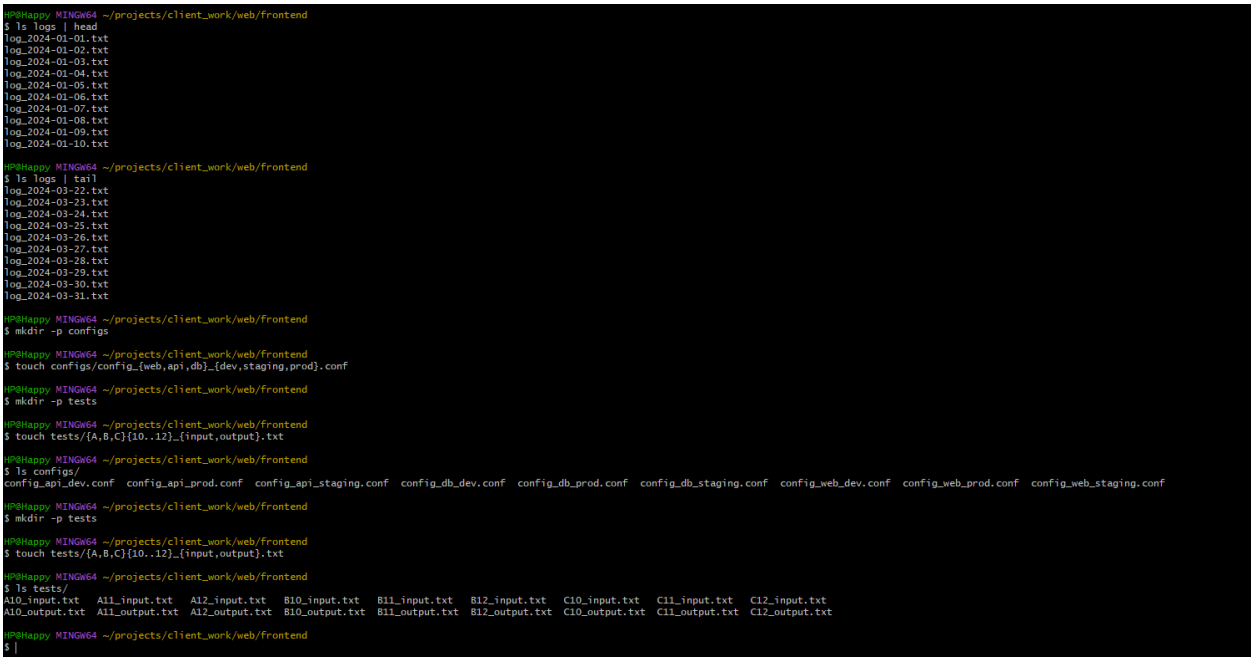
4.

```
HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls web/html | wc -l
3

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls web/css | wc -l
8

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls web/js | wc -l
6

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls web/backups | wc -l
20

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$
```

5.

```
HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls
ab.md  archive/  cat.js  image2.png  page_001.html  projects/  style.css  style_mobile.css  web/  xyz.py

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ mv *[0-9]* archive/

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls archive/
image2.png  page_001.html

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ mkdir -p desktop
shopt -s extglob
cp !(*mobile*|*tablet*).css desktop/
ls desktop/
style.css

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls
ab.md  archive/  cat.js  desktop/  projects/  style.css  style_mobile.css  web/  xyz.py

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls ???.*
cat.js  xyz.py

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls [b-df-hj-np-tv-zB-DF-HJ-NP-TV-Z]*
cat.js  style.css  style_mobile.css  xyz.py

desktop:
style.css

projects:
clientA/  clientB/  shared/

web:
backups/  css/  html/  js/

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls *.*??
ab.md  cat.js  style.css  style_mobile.css  xyz.py

HP@Happy MINGW64 ~/projects/client_work/web/frontend
```

6.



7. • **Line endings matter**: Scripts or config files may fail on Linux if they contain CR (`^M`) from Windows.

• **Different tools detect differences differently**:

- `cmp`: byte-by-byte
- `diff`: line-by-line text
- `comm`: line-by-line, expects sorted input

Even if files look identical, differences in line endings can cause subtle bugs or misbehavior

```
HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ printf "line1\r\nline2\r\nline3\r\n" > file_windows.txt

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ file_unix.txt
file_windows.txt
bash: file_unix.txt: command not found
bash: file_windows.txt: command not found

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls -l file_unix.txt file_windows.txt
-rw-r--r-- 1 HP 197121 18 Sep 30 17:22 file_unix.txt
-rw-r--r-- 1 HP 197121 21 Sep 30 17:25 file_windows.txt

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ cat file_unix.txt
line1
line2
line3

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ cat file_windows.txt
line1
line2
line3

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ cat -A file_unix.txt
line1$
line2$
line3$

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ cat -A file_windows.txt
line1^M$
line2^M$
line3^M$

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ diff -u file_unix.txt file_windows.txt
--- file_unix.txt       2025-09-30 17:22:10.953186300 +0200
+++ file_windows.txt    2025-09-30 17:25:34.616396500 +0200
@@ -1,3 +1,3 @@
-line1
-line2
-line3
+line1
+line2
+line3

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ cmp file_unix.txt file_windows.txt
file_unix.txt file_windows.txt differ: char 6, line 1
```

8.

```
HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ file_unix.txt     # Linux line endings (LF)
file_windows.txt  # Windows line endings (CRLF)
bash: file_unix.txt: command not found
bash: file_windows.txt: command not found

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ printf "line1\r\nline2\r\nline3\r\n" > file_windows.txt

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ file_unix.txt
file_windows.txt
bash: file_unix.txt: command not found
bash: file_windows.txt: command not found

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ ls -l file_unix.txt file_windows.txt
-rw-r--r-- 1 HP 197121 18 Sep 30 17:22 file_unix.txt
-rw-r--r-- 1 HP 197121 21 Sep 30 17:25 file_windows.txt

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ cat file_unix.txt
line1
line2
line3

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ cat file_windows.txt
line1
line2
line3

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ cat -A file_unix.txt
line1$
line2$
line3$

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ cat -A file_windows.txt
line1^M$
line2^M$
line3^M$

HP@Happy MINGW64 ~/projects/client_work/web/frontend
$ diff -u file_unix.txt file_windows.txt
--- file_unix.txt       2025-09-30 17:22:10.953186300 +0200
+++ file_windows.txt    2025-09-30 17:25:34.616396500 +0200
@@ -1,3 +1,3 @@
-line1
-line2
-line3
+line1
+line2
+line3
```

9.

```
HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ ls
biglog.txt  docs/  errors_with_lineno.txt  hidden_dir/  logs/  scripts/  tmp/

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -exec ls -l {} \; | head
-rw-r--r-- 1 HP 197121 0 Sep 30 17:44 ./.hidden_file
-rw-r--r-- 1 HP 197121 5238 Sep 30 17:47 ./biglog.txt
-rw-r--r-- 1 HP 197121 11 Sep 30 17:44 ./docs/file1.txt
-rw-r--r-- 1 HP 197121 0 Sep 30 17:44 ./docs/file1.txt~
-rw-r--r-- 1 HP 197121 0 Sep 30 17:44 ./docs/file2.bak
-rw-r--r-- 1 HP 197121 10240 Sep 30 17:44 ./docs/file2.bin
-rw-r--r-- 1 HP 197121 0 Sep 29 17:44 ./docs/file_24h.txt
-rw-r--r-- 1 HP 197121 0 Sep 28 17:44 ./docs/file_recent.txt
-rw-r--r-- 1 HP 197121 290 Sep 30 17:47 ./errors_with_lineno.txt
-rw-r--r-- 1 HP 197121 0 Sep 20 17:44 ./logs/old_log.log
find: 'ls' terminated by signal 13
ls: write error: Permission denied
ls: write error: Permission denied
```

10.

```
HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -exec chmod 644 {} \;

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -perm /111 -exec chmod 755 {} \;

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -mtime +30 -print > old_files_list.txt

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -mtime +30 -print0 | xargs -0 du -ch | tail -n1
82K     total

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -name '*.conf' -print

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -name '*.conf' -exec cp {} {}.backup \;

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -name '*.tmp' -atime +30 -print

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -name '*.tmp' -atime +30 -ok rm {} \;

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ ls
biglog.txt  docs/  errors_with_lineno.txt  hidden_dir/  logs/  old_files_list.txt  scripts/  tmp/

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f ! -perm /111 -exec chmod 644 {} \;

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -perm /111 -exec chmod 755 {} \;

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -mtime +30 -exec du -ch {} + | grep total$

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ find . -type f -name "*.conf" -exec cp {} {}.backup \;
```

These commands automate file maintenance tasks effectively using the `find` command and `-exec` option.

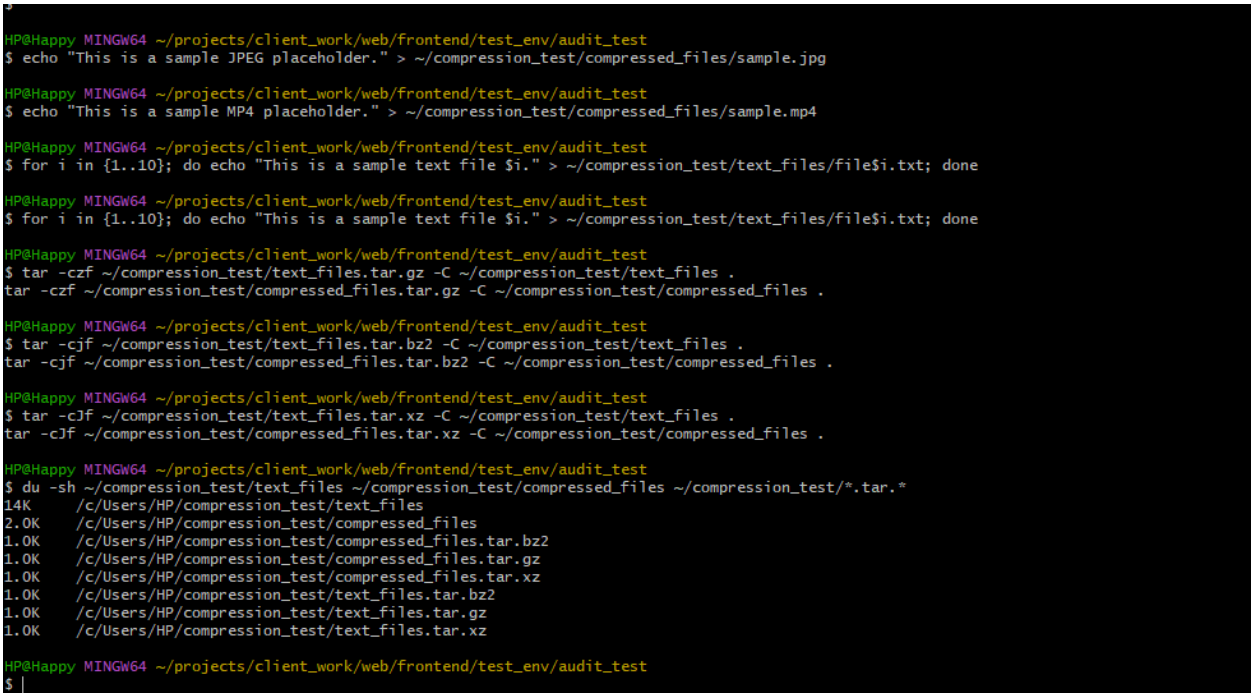
11.

1. **Calculate Compression Ratios:**
   You can calculate the compression ratio using:

   Compression Ratio=Original SizeCompressed Size\text{Compression Ratio} = \frac{\text{Original Size}}{\text{Compressed Size}}Compression Ratio=Compressed SizeOriginal Size

Recommendations for Automated Backups

- **For text files:** Use `tar` with gzip as it typically offers a good balance between speed and compression efficiency.
- **For already-compressed files:** Just archive them without additional compression, as they won't benefit from further compression.



12.

Here I created the directory

Extracted the file and listed the contents of the extracted directory

```
HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ mkdir -p ~/archives

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ echo "This is a sample text file." > ~/archives/sample.txt

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ zip ~/archives/documents.zip ~/archives/sample.txt
bash: zip: command not found

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ echo "This is a sample text file." > ~/archives/sample.txt

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ tar -czf ~/archives/documents.tar.gz -C ~/archives sample.txt

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ tar -tf ~/archives/documents.tar.gz
sample.txt

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ tar -xzf ~/archives/documents.tar.gz -C ~/extracted_files/ sample.txt
tar: /c/Users/HP/extracted_files: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ mkdir -p ~/extracted_files

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ tar -xzf ~/archives/documents.tar.gz -C ~/extracted_files/ sample.txt

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$ ls ~/extracted_files
sample.txt

HP@Happy MINGW64 ~/projects/client_work/web/frontend/test_env/audit_test
$
```

13.

Backup Rotation Strategy

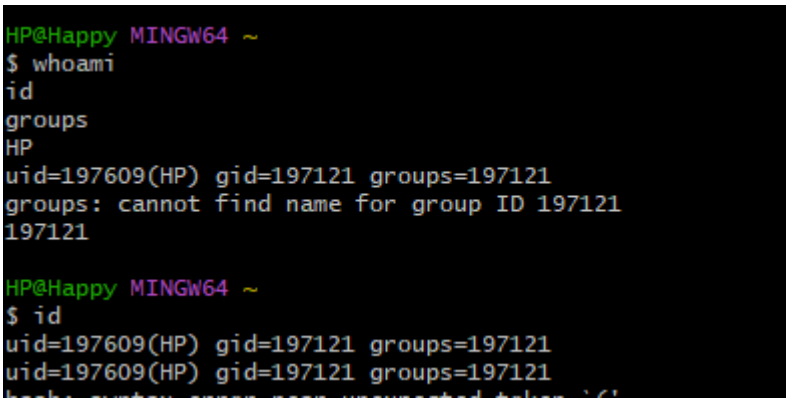
1. **Daily Incremental Backups:** Capture changes made since the last backup.
2. **Weekly Full Backups:** Create a complete snapshot of the server.
3. **Monthly Archives:** Store full backups for long-term retention.
4. **Automatic Cleanup:** Remove old backups to manage storage efficiently.

Backup Schedule

- **Daily Incremental Backups:** Run every night at 2 AM.
- **Weekly Full Backups:** Run every Sunday at 3 AM.
- **Monthly Archives:** Run on the first day of the month at 4 AM.

```
HP@Happy MINGW64 ~
$ mkdir -p ~/test_data
echo "hello world" > ~/test_data/file1.txt
echo "backup demo" > ~/test_data/file2.txt

HP@Happy MINGW64 ~
$ tar -czpf ~/backup-full-$(date +%F).tar.gz ~/test_data
tar: Removing leading `/' from member names

HP@Happy MINGW64 ~
$ ls -lh ~ | grep backup-full
-rw-r--r-- 1 HP 197121  211 Sep 30 20:53 backup-full-2025-09-30.tar.gz

HP@Happy MINGW64 ~
$ tar -tvf ~/backup-full-$(date +%F).tar.gz
drwxr-xr-x HP/197121         0 2025-09-30 20:53 c/Users/HP/test_data/
-rw-r--r-- HP/197121        12 2025-09-30 20:53 c/Users/HP/test_data/file1.txt
-rw-r--r-- HP/197121        12 2025-09-30 20:53 c/Users/HP/test_data/file2.txt

HP@Happy MINGW64 ~
$ tar -tzf ~/backup-full-$(date +%F).tar.gz > /dev/null && echo "Archive OK"
Archive OK

HP@Happy MINGW64 ~
$ mkdir -p ~/restore_test
tar -xvpf ~/backup-full-$(date +%F).tar.gz -C ~/restore_test
c/Users/HP/test_data/
c/Users/HP/test_data/file1.txt
c/Users/HP/test_data/file2.txt

HP@Happy MINGW64 ~
$ ls -l ~/restore_test/test_data
ls: cannot access '/c/Users/HP/restore_test/test_data': No such file or directory

HP@Happy MINGW64 ~
$ tar -tvf ~/backup-full-$(date +%F).tar.gz
drwxr-xr-x HP/197121         0 2025-09-30 20:53 c/Users/HP/test_data/
-rw-r--r-- HP/197121        12 2025-09-30 20:53 c/Users/HP/test_data/file1.txt
-rw-r--r-- HP/197121        12 2025-09-30 20:53 c/Users/HP/test_data/file2.txt

HP@Happy MINGW64 ~
$ mkdir -p ~/restore_test
tar -xvpf ~/backup-full-$(date +%F).tar.gz -C ~/restore_test --strip-components=3
c/Users/HP/test_data/
c/Users/HP/test_data/file1.txt
c/Users/HP/test_data/file2.txt

HP@Happy MINGW64 ~
$ ls -l ~/restore_test/test_data
total 2
-rw-r--r-- 1 HP 197121 12 Sep 30 20:53 file1.txt
-rw-r--r-- 1 HP 197121 12 Sep 30 20:53 file2.txt

HP@Happy MINGW64 ~
$
```

14.


HP@Happy MINGW64 ~
$ whoami
id
groups
HP
uid=197609(HP) gid=197121 groups=197121
groups: cannot find name for group ID 197121
197121
HP@Happy MINGW64 ~
$ id
uid=197609(HP) gid=197121 groups=197121
uid=197609(HP) gid=197121 groups=197121

```
HP@Happy MINGW64 ~
$ whoami
HP

HP@Happy MINGW64 ~
$ groups
groups: cannot find name for group ID 197121
197121

HP@Happy MINGW64 ~
$ groups testuser
groups: ‘testuser’: no such user

HP@Happy MINGW64 ~
$ sudo adduser testuser
bash: sudo: command not found

HP@Happy MINGW64 ~
$ net user testuser password /add
The syntax of this command is:

NET USER
[username [password | *] [options]] [/DOMAIN]
         username {password | *} /ADD [options] [/DOMAIN]
         username [/DELETE] [/DOMAIN]
         username [/TIMES:{times | ALL}]
         username [/ACTIVE: {YES | NO}]


HP@Happy MINGW64 ~
$ net user testuser
The user name could not be found.

More help is available by typing NET HELPMSG 2221.


HP@Happy MINGW64 ~
$ net user

User accounts for \\HAPPY

-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
HP                       WDAGUtilityAccount
The command completed successfully.


HP@Happy MINGW64 ~
$
```

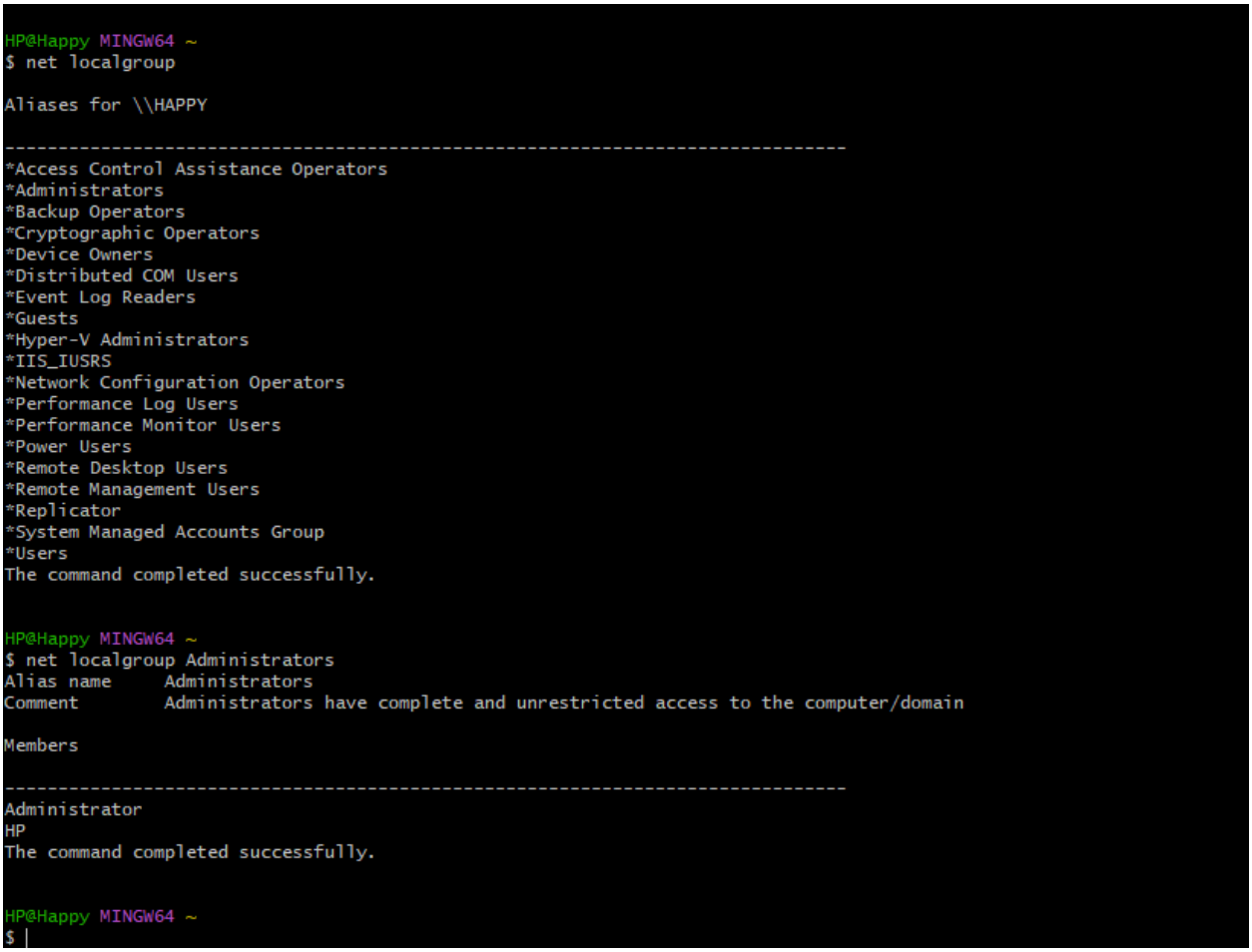
15.

```
HP@Happy MINGW64 ~
$ net user HP
User name                    HP
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            9/30/2025 9:08:38 PM
Password expires             Never
Password changeable          9/30/2025 9:08:38 PM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   9/30/2025 8:39:53 PM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.


HP@Happy MINGW64 ~
$ net localgroup

Aliases for \\HAPPY

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
```

```
HP@Happy MINGW64 ~
$ net localgroup

Aliases for \\HAPPY

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Remote Management Users
*Replicator
*System Managed Accounts Group
*Users
The command completed successfully.


HP@Happy MINGW64 ~
$ net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
HP
The command completed successfully.


HP@Happy MINGW64 ~
$ net localgroup newgroupname /add
The syntax of this command is:

NET LOCALGROUP
[groupname [/COMMENT:"text"]] [/DOMAIN]
             groupname {/ADD [/COMMENT:"text"] | /DELETE}  [/DOMAIN]
             groupname name [...] {/ADD | /DELETE} [/DOMAIN]


HP@Happy MINGW64 ~
```

16.

```
HP@Happy MINGW64 ~
$ net user HP
User name                    HP
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            9/30/2025 9:13:40 PM
Password expires             Never
Password changeable          9/30/2025 9:13:40 PM
Password required            No
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   9/30/2025 8:39:53 PM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *None
The command completed successfully.


HP@Happy MINGW64 ~
$ net localgroup

Aliases for \\HAPPY

-------------------------------------------------------------------------------
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Remote Management Users
*Replicator
*System Managed Accounts Group
*Users
The command completed successfully.
```


HP@Happy MINGW64 ~
$ net localgroup
Aliases for \\HAPPY
*Access Control Assistance Operators
*Administrators
*Backup Operators
*Cryptographic Operators
*Device Owners
*Distributed COM Users
*Event Log Readers
*Guests
*Hyper-V Administrators
*IIS_IUSRS
*Network Configuration Operators
*Performance Log Users
*Performance Monitor Users
*Power Users
*Remote Desktop Users
*Remote Management Users
*Replicator
*System Managed Accounts Group
*Users
The command completed successfully.
HP@Happy MINGW64 ~
$ net localgroup Administrators
Alias name Administrators
Comment Administrators have complete and unrestricted access to the computer/domain
Members
Administrator
HP
The command completed successfully.
HP@Happy MINGW64 ~
$

17.

```
HP@Happy MINGW64 ~
$ mkdir -p ~/forensic_analysis/{regular_files,dirs,symbolic_links,hard_links,device_files,permission_tests,archives}

HP@Happy MINGW64 ~
$ touch ~/forensic_analysis/regular_files/file1.txt
touch ~/forensic_analysis/regular_files/file2.log
echo "Sample log data" > ~/forensic_analysis/regular_files/file2.log

HP@Happy MINGW64 ~
$ mkdir ~/forensic_analysis/dirs/subdir1
mkdir ~/forensic_analysis/dirs/subdir2

HP@Happy MINGW64 ~
$ ln -s ~/forensic_analysis/regular_files/file1.txt ~/forensic_analysis/symbolic_links/link_to_file1

HP@Happy MINGW64 ~
$ ln ~/forensic_analysis/regular_files/file2.log ~/forensic_analysis/hard_links/hard_link_to_file2

HP@Happy MINGW64 ~
$ sudo mknod ~/forensic_analysis/device_files/my_device c 1 3  # Example for a character device
bash: sudo: command not found

HP@Happy MINGW64 ~
$ mkdir -p ~/forensic_analysis/regular_files
echo "Sample log data" > ~/forensic_analysis/regular_files/file1.txt
echo "Sample log data" > ~/forensic_analysis/regular_files/file2.log

HP@Happy MINGW64 ~
$ mkdir -p ~/forensic_analysis/dirs/subdir1
mkdir -p ~/forensic_analysis/dirs/subdir2

HP@Happy MINGW64 ~
$ ln -s ~/forensic_analysis/regular_files/file1.txt ~/forensic_analysis/symbolic_links/link_to_file1
ln: failed to create symbolic link '/c/Users/HP/forensic_analysis/symbolic_links/link_to_file1': File exists

HP@Happy MINGW64 ~
$ rm ~/forensic_analysis/symbolic_links/link_to_file1

HP@Happy MINGW64 ~
$ ln -s ~/forensic_analysis/regular_files/file1.txt ~/forensic_analysis/symbolic_links/link_to_file1

HP@Happy MINGW64 ~
$
```