جامعة قطر
QATAR UNIVERSITY

OS-Project Phase 1

Anas Madkoor 202104114

Faisal Elbadri 202107288

Rashid Nafwa 201912873

Name	Tasks	Percentage
Anas Madkoor	Server-Side Tasks (VM1): Task 1, Task 2, Task 3	33.3%
Faisal Elbadri	Client-side Tasks (VM2) and (VM3): Task 1 and task 2	33.3%
Rashid Nafwa	Client-side Tasks (VM2) and (VM3): Task 2 and task 3	33.3%

GitHub repository: https://github.com/C974/Operating-System-Project

Task 1:

1.1: Create User (Client 1) = server

```
anas@anas-VMware-Virtual-Platform: ~
anas@anas-VMware-Virtual-Platform:~$ sudo adduser client1
[sudo] password for anas:
info: Adding user `client1' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `client1' (1001) ...
info: Adding new user `client1' (1001) with group `client1 (1001)' ...
info: Creating home directory `/home/client1' ...
info: Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
Sorry, passwords do not match.
New password:
BAD PASSWORD: The password fails the dictionary check - it is too simplistic/systematic
Retype new password:
Sorry, passwords do not match.
passwd: Have exhausted maximum number of retries for service
passwd: password unchanged
Try again? [y/N] N
Changing the user information for client1
Enter the new value, or press ENTER for the default
        Full Name []: client 1
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `client1' to supplemental / extra groups `users' ...
info: Adding user `client1' to group `users' ...
anas@anas-VMware-Virtual-Platform:~$
```

Password of client 1 (SFTP): **Os-project!12345**

Verify the creation of client 1

```
anas@anas-VMware-Virtual-Platform:~$ cat /etc/passwd | grep '/home'
anas:x:1000:1000:anas:/home/anas:/bin/bash
client1:x:1001:1001:client 1,,,:/home/client1:/bin/bash
```

1.2: Install and Enable SSHD

جامعة قطر
QATAR UNIVERSITY

```
anas@anas-VMware-Virtual-Platform:~$ sudo apt update
Hit:1 http://qa.archive.ubuntu.com/ubuntu noble InRelease
Get:2 http://qa.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Get:3 http://qa.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Get:4 http://qa.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [599 kB]
Get:5 http://qa.archive.ubuntu.com/ubuntu noble-updates/main i386 Packages [318 kB]
Get:6 http://qa.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [147 kB]
Get:7 http://qa.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [114 kB
```

```
anas@anas-VMware-Virtual-Platform:~$ sudo apt install openssh-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
```

```
anas@anas-VMware-Virtual-Platform:~$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/system
d-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink /etc/systemd/system/sshd.service → /usr/lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /usr/lib/syste
md/system/ssh.service.
anas@anas-VMware-Virtual-Platform:~$ sudo systemctl start ssh
anas@anas-VMware-Virtual-Platform:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Wed 2024-10-30 13:14:52 +03; 40s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 4765 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 4767 (sshd)
      Tasks: 1 (limit: 19051)
     Memory: 1.2M (peak: 1.5M)
        CPU: 30ms
     CGroup: /system.slice/ssh.service
             └─4767 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 30 13:14:52 anas-VMware-Virtual-Platform systemd[1]: Starting ssh.service - OpenBSD>
Oct 30 13:14:52 anas-VMware-Virtual-Platform sshd[4767]: Server listening on :: port 22.
Oct 30 13:14:52 anas-VMware-Virtual-Platform systemd[1]: Started ssh.service - OpenBSD >
```

Inside the server we created client 2 client 3 with **Os-project!12345, password**

```
┌──(client1㉿kali)-[~]
└─$ sudo adduser client2
info: Adding user `client2' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `client2' (1002) ...
info: Adding new user `client2' (1002) with group `client2 (1002)' .
..
warn: The home directory `/home/client2' already exists.  Not touchi
ng this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for client2
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `client2' to supplemental / extra groups `user
s' ...
info: Adding user `client2' to group `users' ...

┌──(client1㉿kali)-[~]
└─$ sudo adduser client3
info: Adding user `client3' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `client3' (1003) ...
info: Adding new user `client3' (1003) with group `client3 (1003)' .
..
warn: The home directory `/home/client3' already exists.  Not touchi
ng this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for client3
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
info: Adding new user `client3' to supplemental / extra groups `user
s' ...
info: Adding user `client3' to group `users' ...
```

Configured static ip address for client 2 and client 3,

┌──(client1㉿kali)-[~]

└─$ sudo nano /etc/network/interfaces

```
  GNU nano 8.2                /etc/network/interfaces *
# This file describes the network interfaces availab
# and how to activate them. For more information, se

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback


# Configuration for client2
auto eth0:0
iface eth0:0 inet static
    address 192.168.15.130
    netmask 255.255.255.0

# Configuration for client3
auto eth0:1
iface eth0:1 inet static
    address 192.168.15.131
    netmask 255.255.255.0
```

Verifying the ip addresses using ip a command on the server which we'll need in task 3

```
┌──(client1㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel s
tate UP group default qlen 1000
    link/ether 00:0c:29:eb:c2:3c brd ff:ff:ff:ff:ff:ff
    inet 192.168.15.129/24 brd 192.168.15.255 scope global dynamic n
oprefixroute eth0
       valid_lft 1430sec preferred_lft 1430sec
    inet 192.168.15.130/24 brd 192.168.15.255 scope global secondary
 eth0:0
       valid_lft forever preferred_lft forever
    inet 192.168.15.131/24 brd 192.168.15.255 scope global secondary
 eth0:1
       valid_lft forever preferred_lft forever
    inet6 fe80::e5e2:6111:bea7:b193/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Modify SSH Configuration for SFTP Access

```
# override default of no subsystems
Subsystem       sftp    /usr/lib/openssh/sftp-server

Match User client1,client2
    ChrootDirectory %h
    ForceCommand internal-sftp
    AllowTcpForwarding no
```

Task 2:

2.1 SSH and SFTP Configuration:

```
  libgfrpc0                    librados2
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 175

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl enable ssh

Synchronizing state of ssh.service with SysV service script with /usr/lib/sys
temd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl start ssh


┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nano /etc/ssh/sshd_config
```

sudo nano /etc/ssh/sshd_config

```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
```

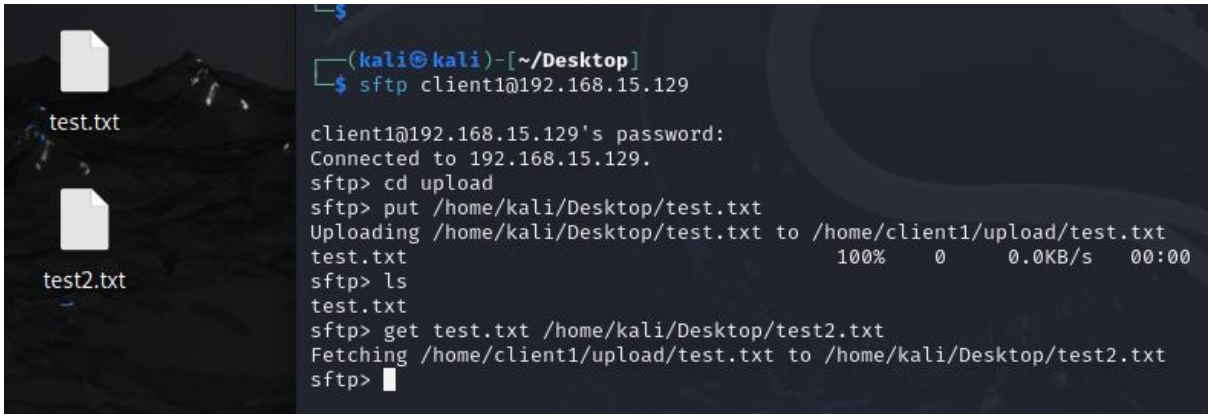
```
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
PermitRootLogin no
ChallengeResponseAuthentication no
UsePAM yes
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl start ssh

┌──(kali㉿kali)-[~/Desktop]
└─$ sudo systemctl status ssh

● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: d>
     Active: active (running) since Wed 2024-10-30 10:40:22 EDT; 4min 45s ago
 Invocation: 8ee890269b3149399bd093f326005f60
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 18926 (sshd)
      Tasks: 1 (limit: 9427)
     Memory: 1.1M (peak: 19.7M)
        CPU: 156ms
     CGroup: /system.slice/ssh.service
             └─18926 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startup>

Oct 30 10:40:34 kali sshd-session[18978]: pam_unix(sshd:session): session cl>
```

Created file with “touch test.txt” on my Desktop then we sftped to the server and uploaded the file, we used ls command on the server to verify that the file was uploaded successfully.

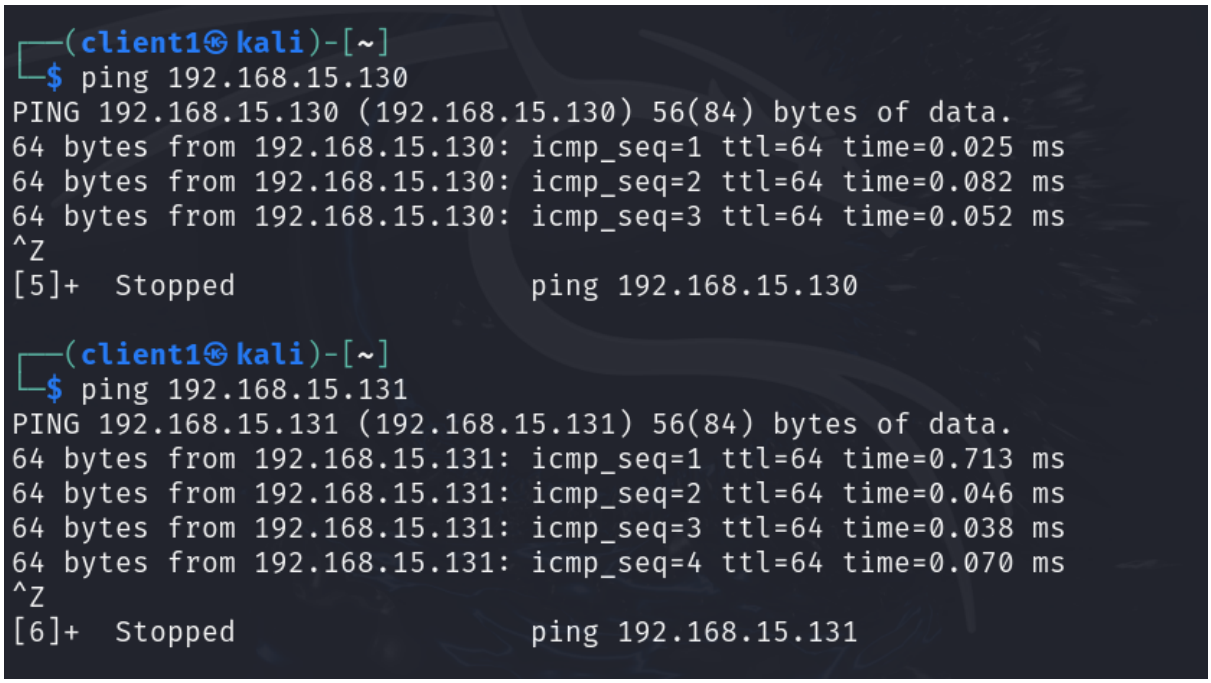
```
┌──(kali㉿kali)-[~/Desktop]
└─$ pwd
/home/kali/Desktop

┌──(kali㉿kali)-[~/Desktop]
└─$

┌──(kali㉿kali)-[~/Desktop]
└─$ sftp client1@192.168.15.129

client1@192.168.15.129's password:
Connected to 192.168.15.129.
sftp> cd upload
sftp> put /home/kali/Desktop/test.txt
Uploading /home/kali/Desktop/test.txt to /home/client1/upload/test.txt
test.txt                                      100%    0     0.0KB/s   00:00
sftp> ls
test.txt
sftp>
```

Now after we have the file uploaded, we downloaded it from the server to desktop while renaming it to test2.txt



Task3:

Pinging client 2 192.168.15.130 and client 3 192.168.131 that we configured the static ips in task 1



Created network.sh

```
  GNU nano 8.2                    network.sh
#!/bin/bash

# Define target IPs
TARGET_IPS=("$@")

# Log file
LOGFILE="network.log"

# Function to check and install necessary tools
install_tools() {
    echo "Checking for required tools ... "
    for tool in ping traceroute; do
        if ! command -v $tool &> /dev/null; then
            echo "$tool not found, installing ... "
            sudo apt-get update
            sudo apt-get install -y $tool
        fi
    done
}

# Function to test connectivity
test_connectivity() {
    for target_ip in "${TARGET_IPS[@]}"; do
                        [ Read 42 lines ]
^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

Created tracroute.sh

```
  GNU nano 8.2                    traceroute.sh
#!/bin/bash

TARGET_IP="$1"
LOGFILE="network.log"

# Function to check the routing table and perform traceroute
check_traceroute() {
    echo "Checking routing table ... " | tee -a "$LOGFILE"
    ip route | tee -a "$LOGFILE"

    echo "Hostname: $(hostname)" | tee -a "$LOGFILE"

    echo "Testing local DNS server ... " | tee -a "$LOGFILE"
    nslookup google.com | tee -a "$LOGFILE"

    echo "Tracing route to google.com ... " | tee -a "$LOGFILE"
    traceroute google.com | tee -a "$LOGFILE"

    echo "Pinging google.com ... " | tee -a "$LOGFILE"
    if ping -c 3 google.com > /dev/null; then
        echo "Successfully pinged google.com." | tee -a "$LOGFILE"
    else
        echo "Failed to ping google.com." | tee -a "$LOGFILE"
```

Changed the privileges of the files to make the executable

```
┌──(client1㉿kali)-[~]
└─$ sudo chmod +x network.sh traceroute.sh
```

Changed privileges to be able to write the network.log file

```
┌──(client1㉿kali)-[~]
└─$ ls
network.sh  traceroute.sh  upload

┌──(client1㉿kali)-[~]
└─$ ls -ld .
drwxr-xr-x 6 root root 4096 Oct 30 12:43 .

┌──(client1㉿kali)-[~]
└─$ sudo chmod +w .
```

Ran the network.sh file using this command sudo ./network.sh "192.168.15.130 192.168.15.131"

Test run 1

```
┌──(client1㉿kali)-[~]
└─$ sudo ./network.sh "192.168.15.130 192.168.15.131"
Checking for required tools ...
Connectivity test run #1
Pinging 192.168.15.130 192.168.15.131 ...
ping: 192.168.15.130 192.168.15.131: Name or service not known
2024-10-30 12:48:13 - 192.168.15.130 192.168.15.131 is not respondin
g.
Checking routing table ...
default via 192.168.15.2 dev eth0 proto dhcp src 192.168.15.129 metr
ic 100
192.168.15.0/24 dev eth0 proto kernel scope link src 192.168.15.129
metric 100
Hostname: kali
Testing local DNS server ...
Server:         192.168.15.2
Address:        192.168.15.2#53

Non-authoritative answer:
Name:   google.com
Address: 192.178.24.238
Name:   google.com
Address: 2a00:1450:4018:80a::200e

Tracing route to google.com ...
traceroute to google.com (192.178.24.238), 30 hops max, 60 byte pack
ets
 1  192.168.15.2 (192.168.15.2)  0.194 ms  0.067 ms  0.228 ms
 2  * * *
```

Test run 2

```
Pinging google.com ...
Successfully pinged google.com.
Connectivity test run #2
Pinging 192.168.15.130 192.168.15.131 ...
ping: 192.168.15.130 192.168.15.131: Name or service not known
2024-10-30 12:48:50 - 192.168.15.130 192.168.15.131 is not respondin
g.
Checking routing table ...
default via 192.168.15.2 dev eth0 proto dhcp src 192.168.15.129 metr
ic 100
192.168.15.0/24 dev eth0 proto kernel scope link src 192.168.15.129
metric 100
Hostname: kali
Testing local DNS server ...
Server:         192.168.15.2
Address:        192.168.15.2#53

Non-authoritative answer:
Name:   google.com
Address: 192.178.24.238
Name:   google.com
Address: 2a00:1450:4018:80a::200e

Tracing route to google.com ...
traceroute to google.com (192.178.24.238), 30 hops max, 60 byte pack
ets
 1  192.168.15.2 (192.168.15.2)  0.094 ms  0.086 ms  0.081 ms
```

Test run 3

```
Connectivity test run #3
Pinging 192.168.15.130 192.168.15.131 ...
ping: 192.168.15.130 192.168.15.131: Name or service not known
2024-10-30 12:49:27 - 192.168.15.130 192.168.15.131 is not respondin
g.
Checking routing table ...
default via 192.168.15.2 dev eth0 proto dhcp src 192.168.15.129 metr
ic 100
192.168.15.0/24 dev eth0 proto kernel scope link src 192.168.15.129
metric 100
Hostname: kali
Testing local DNS server ...
Server:         192.168.15.2
Address:        192.168.15.2#53

Non-authoritative answer:
Name:   google.com
Address: 192.178.24.238
Name:   google.com
Address: 2a00:1450:4018:80a::200e

Tracing route to google.com ...
traceroute to google.com (192.178.24.238), 30 hops max, 60 byte pack
ets
 1  192.168.15.2 (192.168.15.2)  0.111 ms  0.107 ms  0.087 ms
 2  * * *
```

Now we have network.log file which stores the output in the log file

```
Pinging google.com ...
Successfully pinged google.com.

┌──(client1㉿kali)-[~]
└─$ ls
network.log  network.sh  traceroute.sh  upload
```

System.sh:

```
  GNU nano 8.2                    system.sh
#!/bin/bash

# Define log file names
DISK_LOG="disk_info.log"
MEM_CPU_LOG="mem_cpu_info.log"

# Function to gather disk information
function gather_disk_info {
    echo "Disk Information for HOME Directory:" | tee $DISK_LOG
    echo "————————————————————————————————————" | tee -a $DISK_LOG
    du -h --max-depth=1 $HOME | tee -a $DISK_LOG
    echo "" | tee -a $DISK_LOG
    df -h $HOME | tee -a $DISK_LOG
}

# Function to gather memory and CPU information
function gather_mem_cpu_info {
    echo "Memory and CPU Information:" | tee $MEM_CPU_LOG
    echo "———————————————————————————" | tee -a $MEM_CPU_LOG

    # Memory usage
    free -h | awk '/^Mem:/ {printf("Used Memory: %s, Free Memory: %>
    # CPU model and number of cores
                 [ File 'system.sh' is unwritable ]
^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute
```

System.sh, disk_info.log and mem_cpu_info.log files

```
┌──(client1㉿kali)-[~]
└─$ sudo chmod u+w ~

┌──(client1㉿kali)-[~]
└─$ sudo ./system.sh
Disk Information for HOME Directory:
────────────────────────────────────
12K     /root/.local
4.0K    /root/.ssh
4.0K    /root/.cache
64K     /root

Filesystem      Size  Used Avail Use% Mounted on
/dev/sda1        79G   16G   59G  22% /
Memory and CPU Information:
───────────────────────────
Used Memory: 1.2Gi, Free Memory: 957Mi
Model name:                          AMD Ryzen 9 5900HS with Radeon
 Graphics
BIOS Model name:                     AMD Ryzen 9 5900HS with Radeon
 Graphics          CPU @ 3.3GHz
Information gathered successfully!

┌──(client1㉿kali)-[~]
└─$ ls
disk_info.log     network.log  system.sh      upload
mem_cpu_info.log  network.sh   traceroute.sh
```

Zipped the files

```
┌──(client1㉿kali)-[~]
└─$ sudo zip exported_files.zip disk_info.log mem_cpu_info.log netwo
rk.log network.sh system.sh traceroute.sh
  adding: disk_info.log (deflated 35%)
  adding: mem_cpu_info.log (deflated 49%)
  adding: network.log (deflated 89%)
  adding: network.sh (deflated 52%)
  adding: system.sh (deflated 60%)
  adding: traceroute.sh (deflated 55%)

┌──(client1㉿kali)-[~]
└─$ ls
disk_info.log       mem_cpu_info.log  network.sh  traceroute.sh
exported_files.zip  network.log       system.sh   upload
```

Downloaded them in our host machine (kali) in the download folder

```
┌──(kali㉿kali)-[~]
└─$ scp client1_username@192.168.15.130:/home/client1/exported_files.zip ~/Downloads/

The authenticity of host '192.168.15.130 (192.168.15.130)' can't be established.
ED25519 key fingerprint is SHA256:9DUhxCxZYzLOreuOIpCbTKt3X07HEOZKrG3b7H4YpDE.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])?
Host key verification failed.
scp: Connection closed

┌──(kali㉿kali)-[~]
└─$ scp client1@192.168.15.129:/home/client1/exported_files.zip ~/Downloads/

client1@192.168.15.129's password:
exported_files.zip                                    100% 3098     2.1MB/s   00:00
```

Client Machine Setup (VM2 and VM3):

Task 1:

```
┌──(client1㉿kali)-[~]
└─$ ssh -V
OpenSSH_9.9p1 Debian-2, OpenSSL 3.3.2 3 Sep 2024
```

```
┌──(client1㉿kali)-[~]
└─$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; >
     Active: active (running) since Wed 2024-10-30 11:35:29 EDT; 2h>
 Invocation: b38ad4089fc841df9670de5e66a7b98f
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 100572 ExecStartPre=/usr/sbin/sshd -t (code=exited, st>
   Main PID: 100574 (sshd)
      Tasks: 1 (limit: 9427)
     Memory: 4.8M (peak: 23.6M)
        CPU: 651ms
     CGroup: /system.slice/ssh.service
             └─100574 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-1>

Oct 30 13:22:01 kali sshd-session[153537]: pam_unix(sshd:session): >
Oct 30 13:22:01 kali sshd-session[153537]: pam_systemd(sshd:session>
Oct 30 13:22:01 kali sshd-session[153537]: pam_unix(sshd:session): >
Oct 30 13:22:01 kali sshd-session[153537]: pam_systemd(sshd:session>
Oct 30 13:32:46 kali sshd-session[158963]: Connection closed by 192>
Oct 30 13:33:45 kali sshd-session[159344]: pam_unix(sshd:auth): aut>
Oct 30 13:33:47 kali sshd-session[159344]: Failed password for clie>
Oct 30 13:33:55 kali sshd-session[159344]: Accepted password for cl>
```

Install sftp client

```
└─$ sudo apt install openssh-client
openssh-client is already the newest version (1:9.9p1-2).
The following packages were automatically installed and are no longe
r required:
  fonts-liberation2          libimobiledevice6
  freerdp2-x11               libiniparser1
  hydra-gtk                  libjim0.82t64
  ibverbs-providers          libjsoncpp25
  libassuan0                 libmfx1
  libavfilter9               libplacebo338
  libboost-iostreams1.83.0   libplist3
  libboost-thread1.83.0      libpostproc57
  libcephfs2                 librados2
  libfreerdp-client2-2t64    librdmacm1t64
  libfreerdp2-2t64           libusbmuxd6
  libgail-common             libwinpr2-2t64
```

Checking if scp is installed

```
└─$ scp
usage: scp [-346ABCOpqRrsTv] [-c cipher] [-D sftp_server_path] [-F s
sh_config]
           [-i identity_file] [-J destination] [-l limit] [-o ssh_op
tion]
           [-P port] [-S program] [-X sftp_option] source ... target
```

Task 2 configuration:

```
└─$ cat /etc/passwd | grep client
client1:x:1001:1001:,,,:/home/client1:/bin/bash
client2:x:1002:1002:,,,:/home/client2:/bin/bash
client3:x:1003:1003:,,,:/home/client3:/bin/bash
```

Shh to client 2

```
┌──(client1㉿kali)-[~]
└─$ ssh client2@192.168.15.130
The authenticity of host '192.168.15.130 (192.168.15.130)' can't be
established.
ED25519 key fingerprint is SHA256:9DUhxCxZYzLOreuOIpCbTKt3X07HEOZKrG
3b7H4YpDE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
 yes
Could not create directory '/home/client1/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/client1/.ss
h/known_hosts).
client2@192.168.15.130's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2
024-05-30) x86_64

The programs included with the Kali GNU/Linux system are free softwa
re;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Shh from client 2 to client 3

```
┌──(client2㉿kali)-[~]
└─$ ssh client3@192.168.15.131
The authenticity of host '192.168.15.131 (192.168.15.131)' can't be
established.
ED25519 key fingerprint is SHA256:9DUhxCxZYzLOreuOIpCbTKt3X07HEOZKrG
3b7H4YpDE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
 yes
Warning: Permanently added '192.168.15.131' (ED25519) to the list of
 known hosts.
client3@192.168.15.131's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2
024-05-30) x86_64

The programs included with the Kali GNU/Linux system are free softwa
re;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
┌──(client3㉿kali)-[~]
└─$
```

Sftp to client 2

```
└─$ sftp client2@192.168.15.130
The authenticity of host '192.168.15.130 (192.168.15.130)' can't be
established.
ED25519 key fingerprint is SHA256:9DUhxCxZYzLOreuOIpCbTKt3X07HEOZKrG
3b7H4YpDE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
 yes
Could not create directory '/home/client1/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/client1/.ss
h/known_hosts).
client2@192.168.15.130's password:
Connected to 192.168.15.130.
sftp>
```

Sftp to client 3

```
└─$ sftp client3@192.168.15.131
The authenticity of host '192.168.15.131 (192.168.15.131)' can't be
established.
ED25519 key fingerprint is SHA256:9DUhxCxZYzLOreuOIpCbTKt3X07HEOZKrG
3b7H4YpDE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])?
 yes
Could not create directory '/home/client1/.ssh' (Permission denied).
Failed to add the host to the list of known hosts (/home/client1/.ss
h/known_hosts).
client3@192.168.15.131's password:
Connected to 192.168.15.131.
sftp>
```

Task 3 Shell Scripting:

Login.sh in client 2

```
client2@kali: ~
File  Actions  Edit  View  Help
 GNU nano 8.2                    login.sh *
!/bin/bash

 Log file for invalid attempts
NVALID_LOG="invalid_attempts.log"

 Function to log invalid attempts
og_invalid_attempt() {
    local username="$1"
    echo "$(date): Invalid login attempt for user: $username" >> "$>


 Function to perform login
erform_login() {
    local username="$1"
    local password="$2"
    # Try to login via SSH (using a dummy command to simulate)
    if sshpass -p "$password" ssh -o StrictHostKeyChecking=no "$use>
        echo "Login successful for user: $username"
        return 0
    else
        return 1
    fi
```

Check.sh

```
client2@kali: ~
File  Actions  Edit  View  Help
 GNU nano 8.2                    check.sh
#!/bin/bash

# Log file for permission changes
LOG_FILE="perm_change.log"

# Find files with permission 777
echo "Files with permission 777:" | tee -a "$LOG_FILE"
find /path/to/search -type f -perm 777 -exec ls -l {} \; | tee -a ">

# Change permissions from 777 to 700
find /path/to/search -type f -perm 777 -exec chmod 700 {} \; -exec >

echo "Permission changes logged in $LOG_FILE."
```

Then we zipped both login.sh and check.sh

```
┌──(client2㉿kali)-[~]
└─$ sudo chmod +x login.sh check.sh

┌──(client2㉿kali)-[~]
└─$ nano login.sh

┌──(client2㉿kali)-[~]
└─$ ls
check.sh  login.sh  upload

┌──(client2㉿kali)-[~]
└─$ zip scripts.zip check.sh login.sh
  adding: check.sh (deflated 50%)
  adding: login.sh (deflated 54%)

┌──(client2㉿kali)-[~]
└─$ ls
check.sh  login.sh  scripts.zip  upload
```

Downloaded the zip file we just created on our host machine (kali)

```
┌──(kali㉿kali)-[~]
└─$ scp client2@192.168.15.130:~/scripts.zip ~/Downloads/

The authenticity of host '192.168.15.130 (192.168.15.130)' can't be established.
ED25519 key fingerprint is SHA256:9DUhxCxZYzLOreuOIpCbTKt3X07HEOZKrG3b7H4YpDE.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.15.130' (ED25519) to the list of known hosts.
client2@192.168.15.130's password:
scripts.zip                                                   100% 1175   479.8KB/s   00:00
```

Client 3 Side Shell script 1: (Search.sh):

```
client3@kali: ~
File  Actions  Edit  View  Help
  GNU nano 8.2                    search.sh
#!/bin/bash

# Define variables
search_date=$(date +"%Y-%m-%d %H:%M:%S")
bigfile="bigfile"
email="am2104114@qu.edu.qa"

# Find files larger than 1M
find ~ -type f -size +1M > "$bigfile"
count=$(wc -l < "$bigfile")

# Log the search date and number of files found
{
    echo "Search Date: $search_date"
    echo "Number of files larger than 1M: $count"
    echo "Files:"
    cat "$bigfile"
} >> "$bigfile"

# Check if bigfile is not empty and send email
if [ "$count" -gt 0 ]; then
    mail -s "Files larger than 1M found" "$email" < "$bigfile"
fi
                          [ Read 23 lines ]
```

Clientinfo.sh

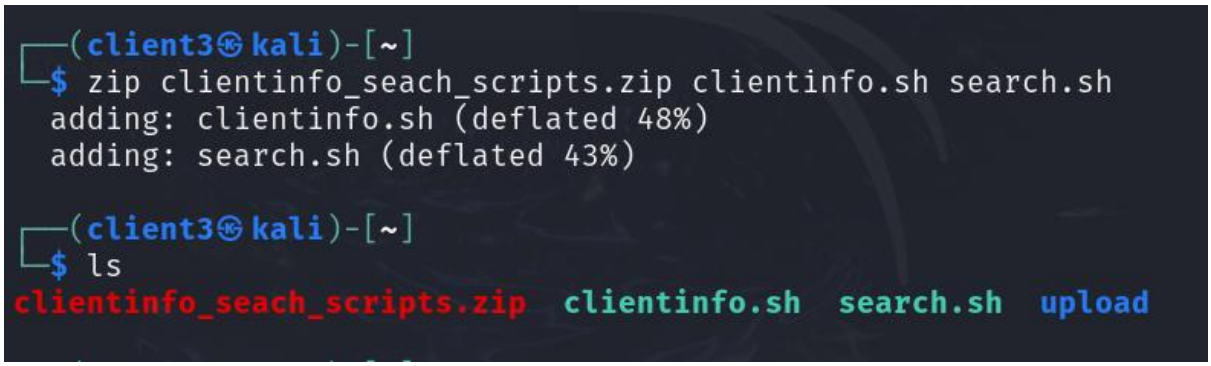
```
client3@kali: ~
File  Actions  Edit  View  Help
  GNU nano 8.2                    clientinfo.sh *
#!/bin/bash
# Define variables
log_file="process_info.log"
server="client1@192.168.15.129"
current_time=$(date +"%Y-%m-%d %H:%M:%S")

# Gather process information
{
    echo "Process Information as of: $current_time"
    echo "═══════════════════════════════"
    echo "Process Tree:"
    ps axjf

    echo -e "\nDead or Zombie Processes:"
    ps aux | grep 'Z'  # Check for zombie processes

    echo -e "\nCPU Usage:"
    top -b -n1 | head -n 10  # Adjust as necessary

    echo -e "\nMemory Usage:"
    free -h  # Display memory usage

    echo -e "\nTop 5 Resource-Consuming Processes:"
^G Help      ^O Write Out ^F Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

To run the script every hour

```
┌──(client3㉿kali)-[~]
└─$ crontab -e
```

0 * * * * /home/client3/clientinfo.sh

Now we zip the files



Now we download the file from kali the host machine