

## TASK 7

Write a script to scan ports 20-25 on a user-supplied IP using 'nc' or 'timeout'.

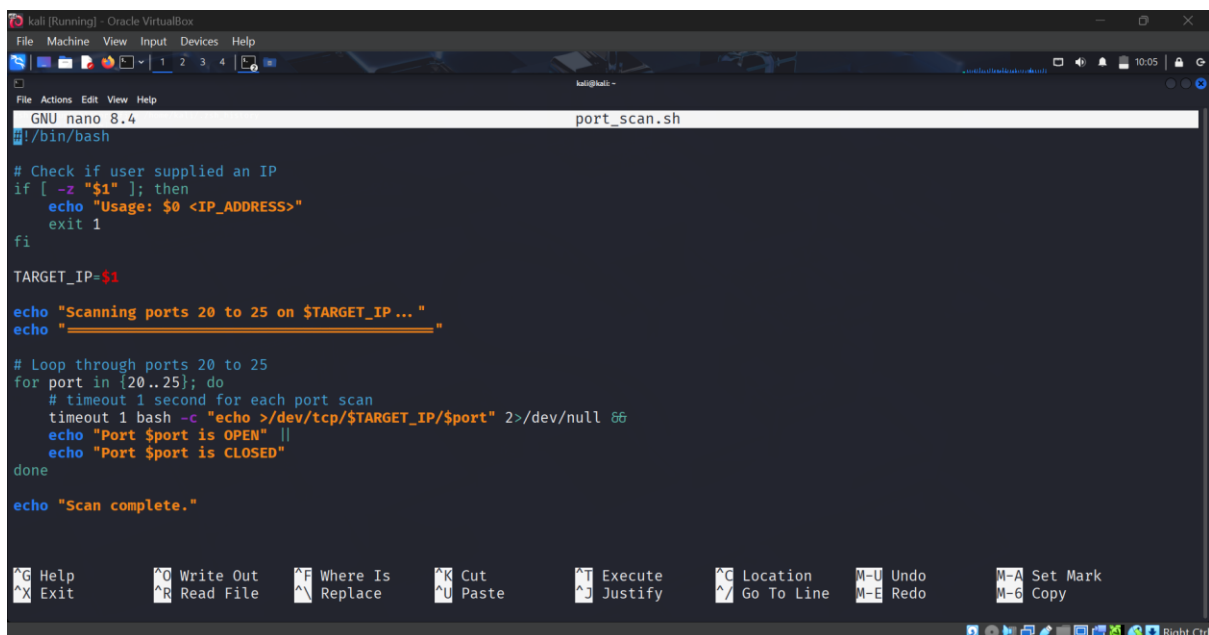
Step 1 :

Create a script

```
(kali@kali)-[~]  
$ nano port_scan.sh
```

Step 2 :

Paste the code



```
GNU nano 8.4 port_scan.sh  
#!/bin/bash  
  
# Check if user supplied an IP  
if [ -z "$1" ]; then  
    echo "Usage: $0 <IP_ADDRESS>"  
    exit 1  
fi  
  
TARGET_IP=$1  
  
echo "Scanning ports 20 to 25 on $TARGET_IP..."  
echo "===== "  
  
# Loop through ports 20 to 25  
for port in {20..25}; do  
    # timeout 1 second for each port scan  
    timeout 1 bash -c "echo >/dev/tcp/$TARGET_IP/$port" 2>/dev/null &&  
    echo "Port $port is OPEN" ||  
    echo "Port $port is CLOSED"  
done  
  
echo "Scan complete."
```

Step 3 :

Make the script executable

```
(kali@kali)-[~]  
$ chmod +x port_scan.sh
```

Step 4 :

Verify the output

```
(kali㉿kali)-[~]  
$ ./port_scan.sh 192.168.1.10  
Scanning ports 20 to 25 on 192.168.1.10 ...  
=====
```

Port 20	is	CLOSED
Port 21	is	CLOSED
Port 22	is	CLOSED
Port 23	is	CLOSED
Port 24	is	CLOSED
Port 25	is	CLOSED

```
Scan complete.  
  
(kali㉿kali)-[~]  
$
```