1. ip addr
2. ping 10.0.0.228
3. ping 10.0.0.71
4. sudo systemctl stop ssh
5. sudo systemctl stop ssh.socket
6. sudo systemctl disable ssh.socket
7. sudo lsof -i
8. sudo ufw disable
9. sudo ufw status
10. sudo bash -c 'while true; do echo -e "HTTP/1.1 200 OK\n\n $(date)" | nc -l -p 80 | tee -a smtp.log; done'
11. while true; do echo -e "220 Welcome to fake FTP server" | nc -l -p 21 | tee -a ftp.log; done
12. while true; do echo -e "SSH-2.0-OpenSSH_7.4" | nc -l -p 22 | tee -a ftp.log; done
13. sudo bash -c 'while true; do echo -e "220 Fake SMTP Server\r\n" | nc -l -p 25 | tee -a smtp.log; done'
14. sudo bash -c 'while true; do echo -e "Welcome to the Telnet server" | nc -l -p 23 | tee -a smtp.log; done'
15. firefox http://10.0.0.71:80
16. curl http://10.0.0.71:80
17. nc 10.0.0.71 21
18. ssh root@10.0.0.71
19. telnet 10.0.0.71 23
20. nc 10.0.2.15 25
21. npmap -p 1-65535 -T4 -A -v 10.0.0.71
22. sudo chmod 644 *.log
23. ls -lh *.log
24. cat smtp.log
25. cat -v smtp.log
26. xxd smtp.log
27. python3 http_server.py
28. python3 echo_server.py

29. curl http://localhost:8080
30. http://10.0.0.71:8080
31. telnet 10.0.0.71 8080
32. telnet 10.0.0.71 9090
33.

```
sudo cat smtp.log
sudo lsof -i -P -n | grep LISTEN
```

```
(ip.addr == 10.0.0.228 || ip.addr == 10.0.0.71) && tcp.port == 25
```

“We observed unexpected or partial inputs in the honeypot logs during nmap scanning. This is consistent with known behavior of service fingerprinting tools, which send malformed or edge-case data to detect service versions or OS types.”