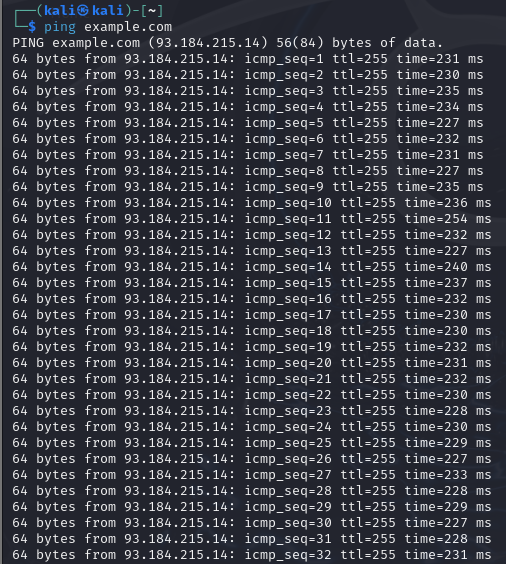
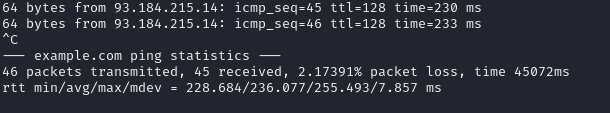
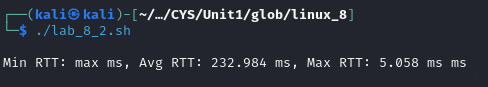
Lab Linux 8

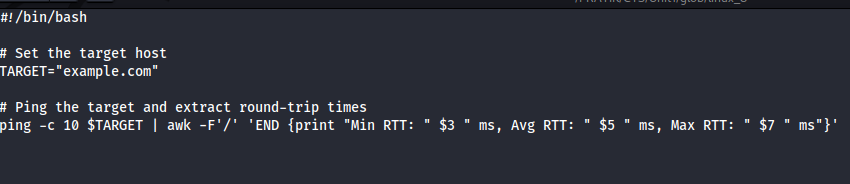
1. Use the ping command to test the connectivity to a remote server (e.g., example.com).



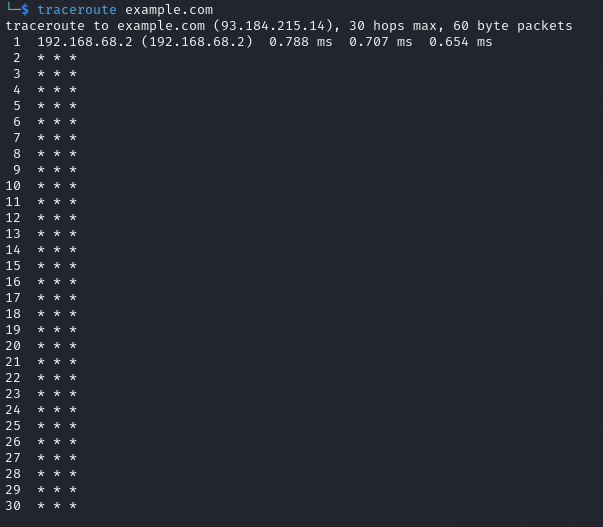


2. Write a script to measure the round-trip time for each packet and analyze the results.





3. Use the traceroute to trace the route packets take to a destination



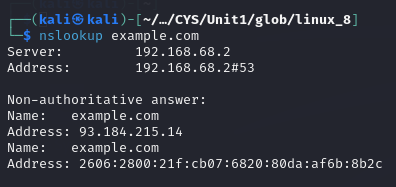
4. Analyze the output to identify any potential bottlenecks or points of failure in the route.

**Analyze Traceroute Output**

When analyzing the output of the traceroute, look for:

* **High Latency**: Identify any hops with significantly higher response times.
* **Timeouts**: Any \* \* \* entries indicate that a hop did not respond. This may suggest a potential bottleneck or a firewall blocking ICMP packets.
* **Consistent Delays**: If a hop consistently shows delays, it could be a point of failure.

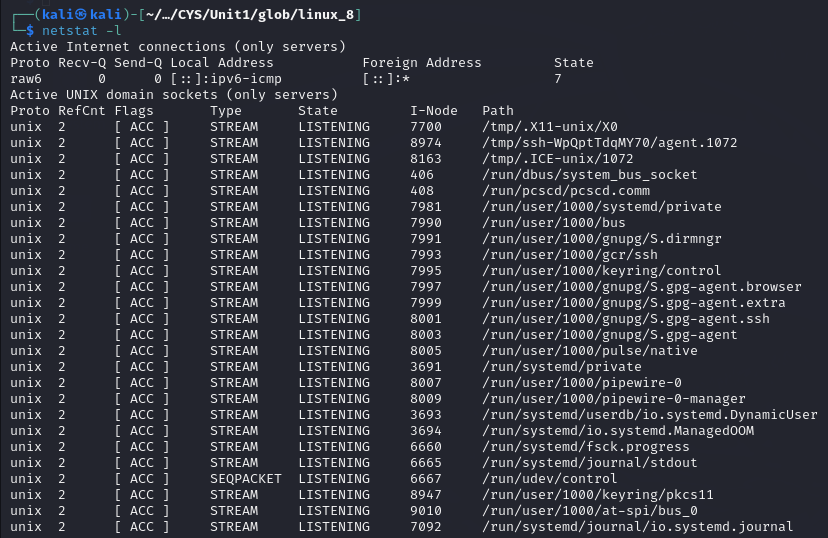
5. Use the nslookup command to find the IP address of a given domain (e.g., example.com).



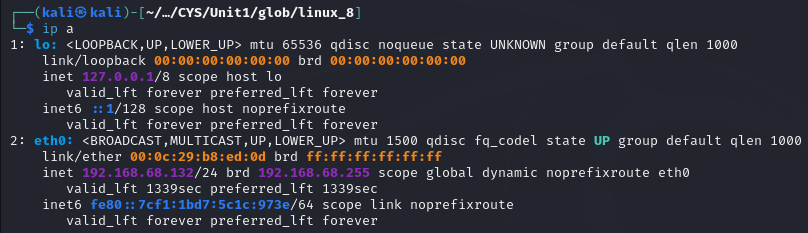
6. Use the netstat command to view active connections and listening ports on your machine.

his command shows:

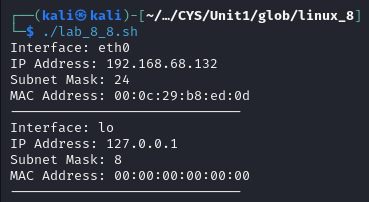
* -t: TCP connections
* -u: UDP connections
* -l: only listening ports
* -n: show numerical addresses instead of resolving hostnames



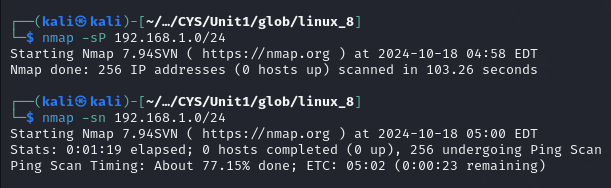
7. Use the ifconfig (Linux) or ip a command to display network interface configurations.



8. Write a script to report document the configuration of each interface, noting the IP address, subnet mask, and any other relevant information.

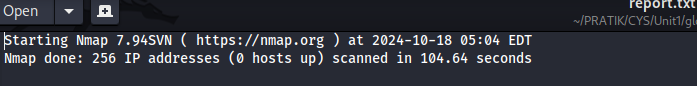


9. Perform a basic network scan using nmap on your local network to identify active devices and open ports.



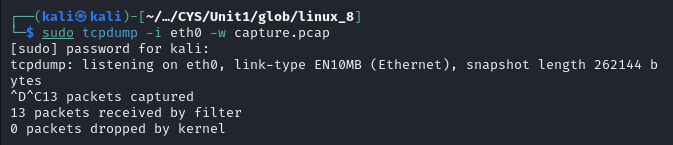
10. Create a report summarizing the devices found, their IP addresses, and the services running on the open ports.



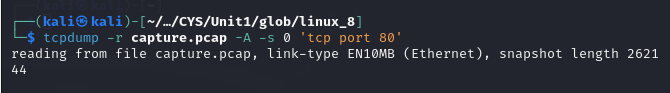


11. Capture network packets using tcpdump on a specific interface.



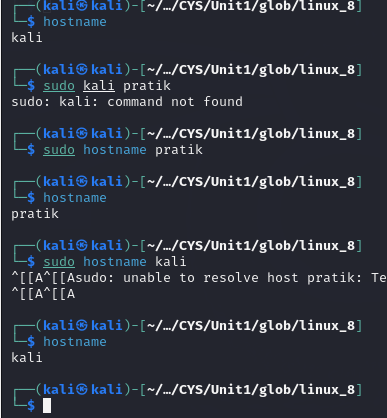


12. Analyze the captured packets for specific protocols (like HTTP or DNS) and summarize your findings.

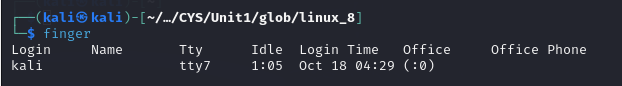


13. Use the whois command to gather registration information about a domain.

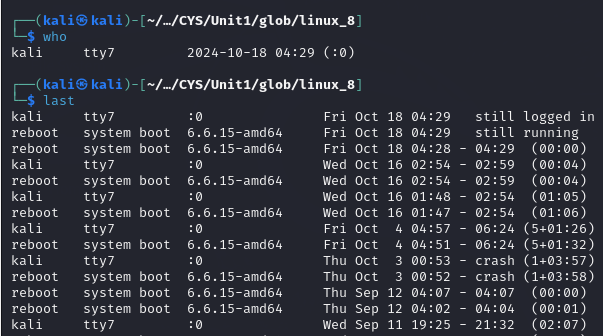
14. Use the hostname command to display and change the hostname of your machine.



15. Use the finger command to gather information about users on a system.

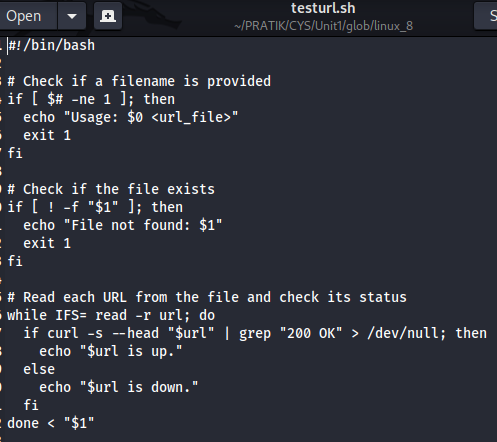


16. Use the who command to see who is currently logged into the system and the last command to view the login history.

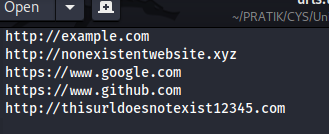


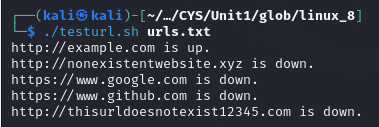
**XARGS**

1. Write a shell script called testurl.sh that accepts a list of urls in a separate file and tests if the website is up or not.

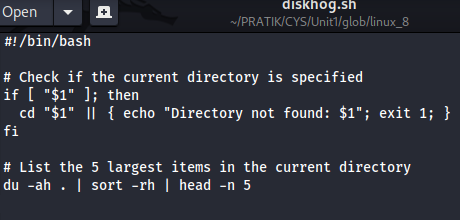


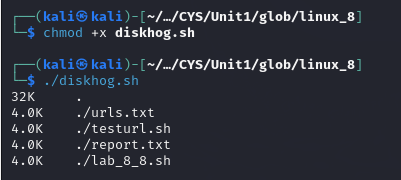




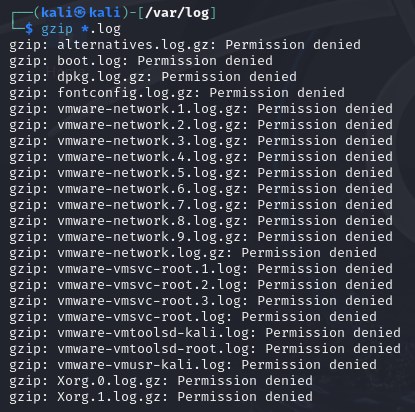


2. Create a shell script called diskhog.sh that lists the 5 largest items (files or directories) in the current directory in decreasing order of size.

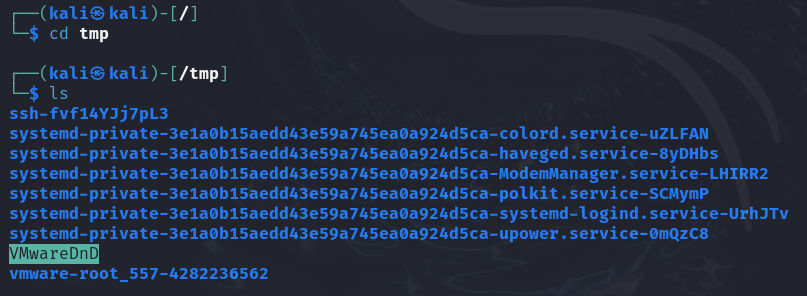


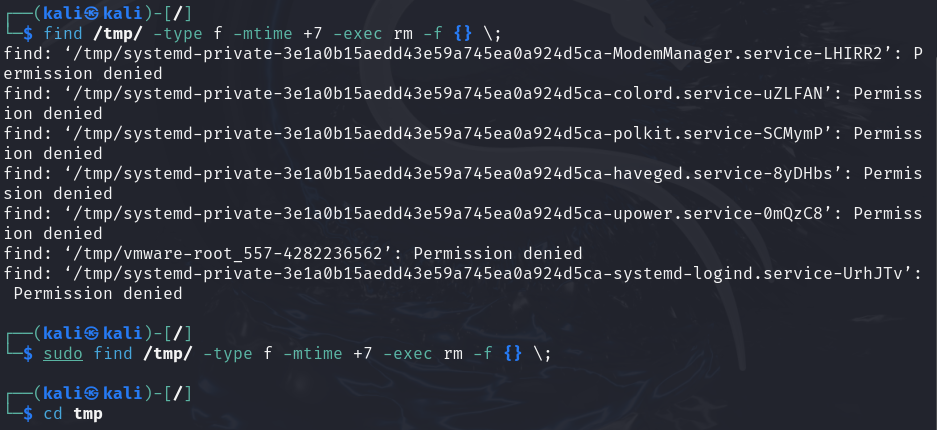


3. compress all .log files found in the /var/logs/ directory?



4. delete all temporary files older than 7 days from the /tmp/ directory?





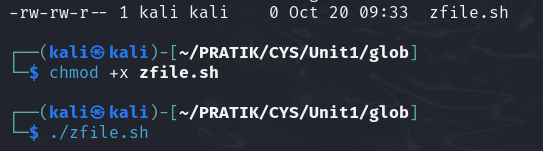
find /tmp/: Searches within the /tmp/ directory.

-type f: Specifies that you're looking for files (not directories).

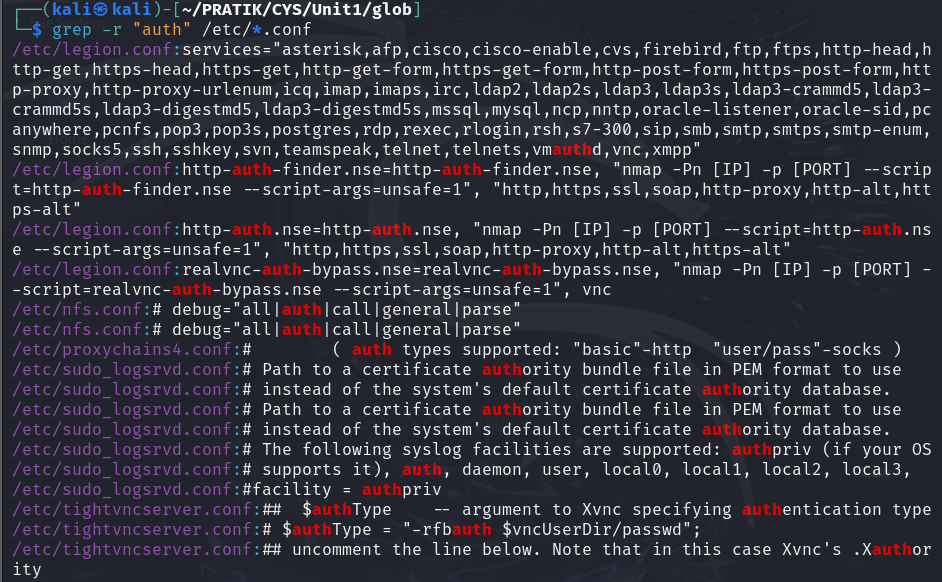
-mtime +7: Finds files that were last modified more than 7 days ago.

-exec rm -f {} \;: For each file found, the rm -f command is executed to forcefully delete the file.

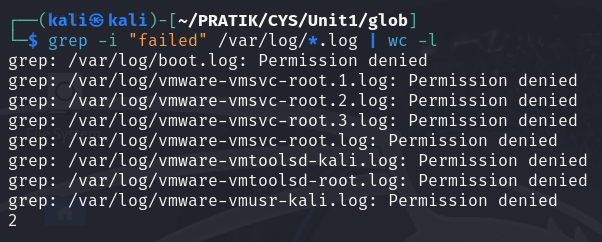
5. write a shell script to make all .sh files in your home directory executable?



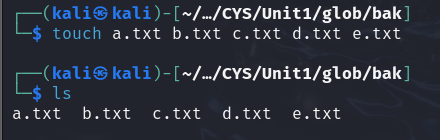
6. search for the string "auth" in all .conf files in the /etc/ directory

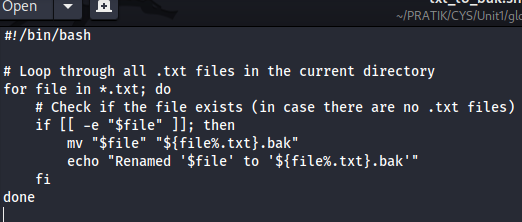


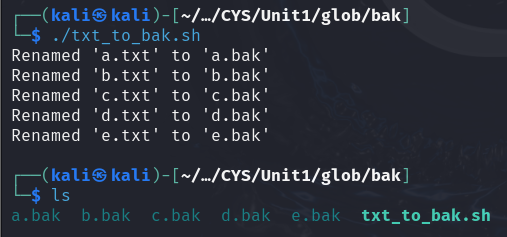
7. count the number of "failed" login attempts in all .log files in /var/log/?



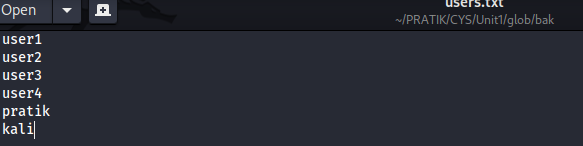
8. rename all .txt files in the current directory by appending .bak

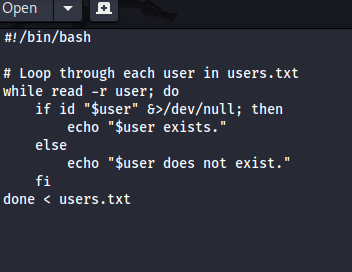


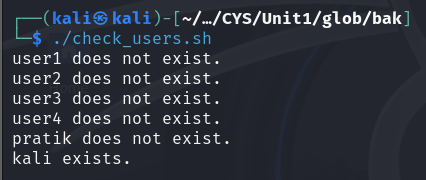




9. Write a shell script to check if a list of users from users.txt exist in the system.







10. search for keywords like "ERROR" or "CRITICAL" in all log files over 1MB in size.

