Assignment 08

Linux os & scripting – b keerthana

AMRUTHESH

241059041

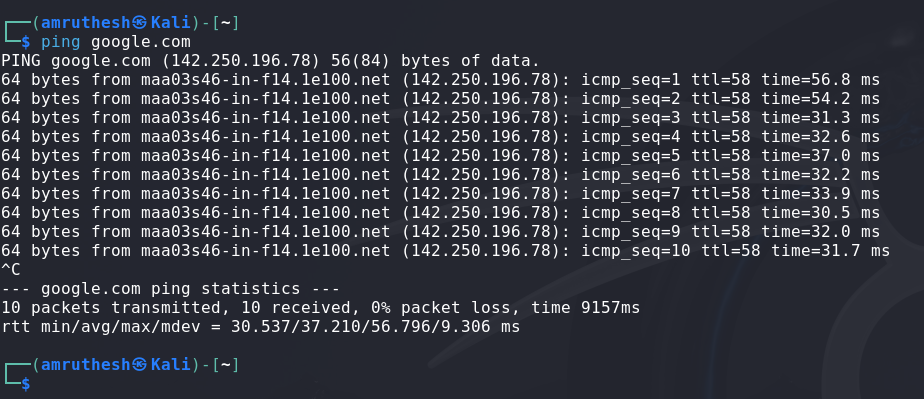
M.E – Cyber Security

MSIS, MANIPAL

**Networking Tasks**

1. **Ping Command**  
   To test connectivity to a remote server:

ping example.com



1. **Script to Measure Round-Trip Time for Each Packet**  
   You can use a bash script to measure round-trip time:

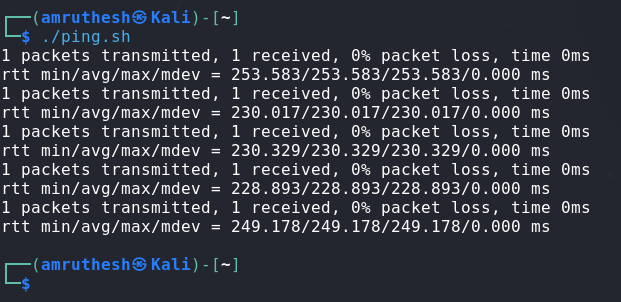
#!/bin/bash

for i in {1..5}

do

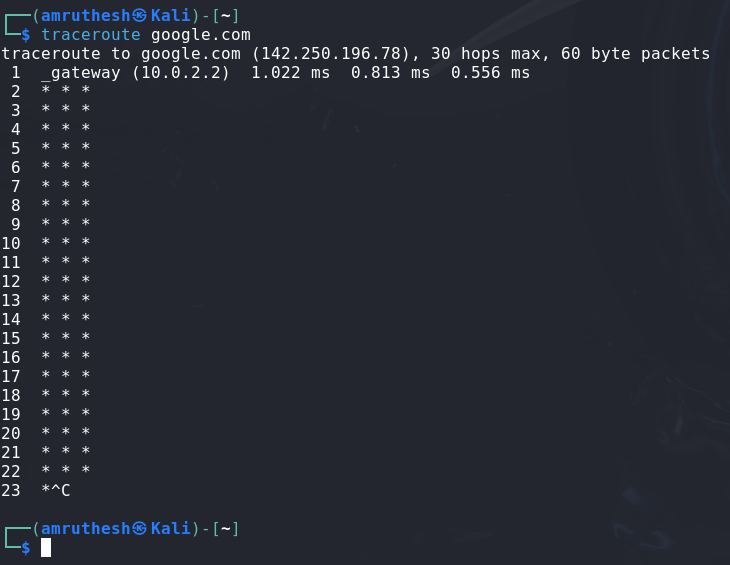
ping -c 1 example.com | tail -n 2

done



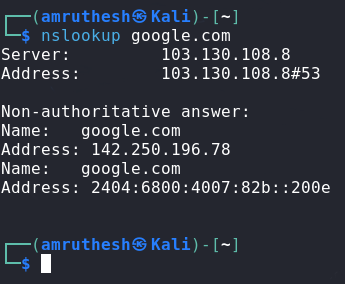
1. **Analyze Traceroute Output for Bottlenecks**  
   Look at the output for any hops that have high latency or timeouts. These might indicate potential bottlenecks or failures.
2. **Traceroute Command**  
   To trace the route packets take to a destination:

traceroute example.com



1. **NSLookup Command**  
   To find the IP address of a domain:

nslookup example.com



1. **Netstat Command**  
   To view active connections and listening ports:

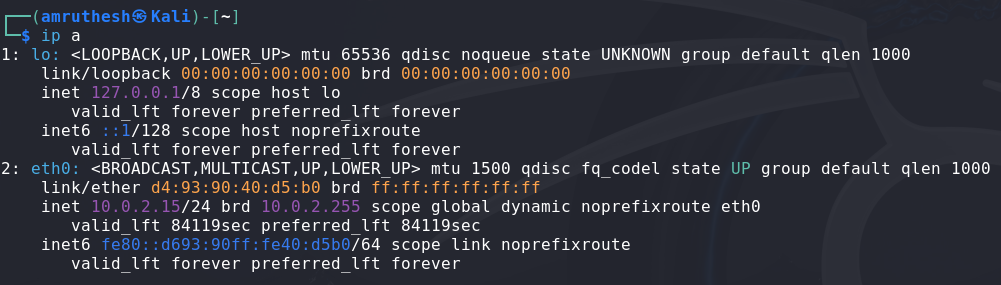
netstat -tuln

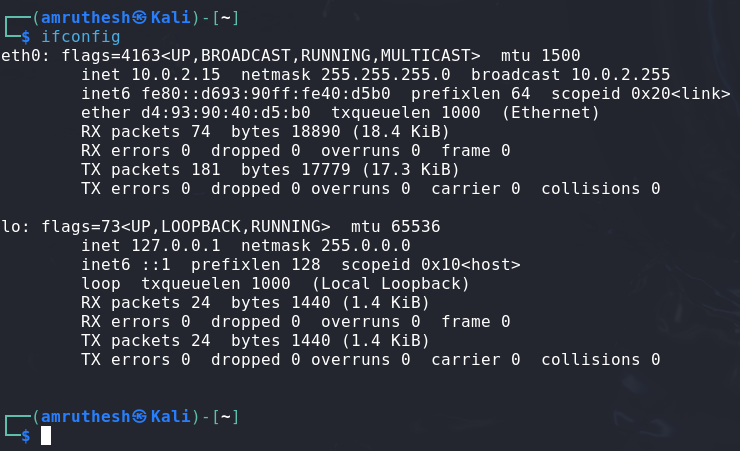


1. **Ifconfig or IP A Command**  
   To display network interface configurations:

Ifconfig or

ip a

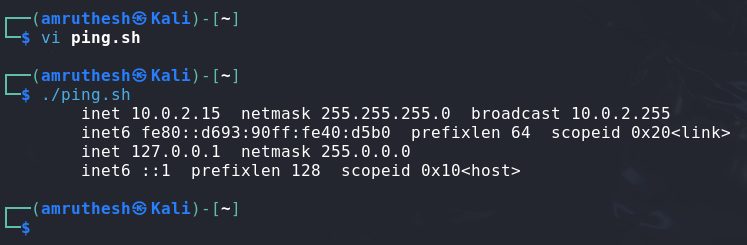




1. **Script to Document Network Interface Configurations**  
   You can create a script like:

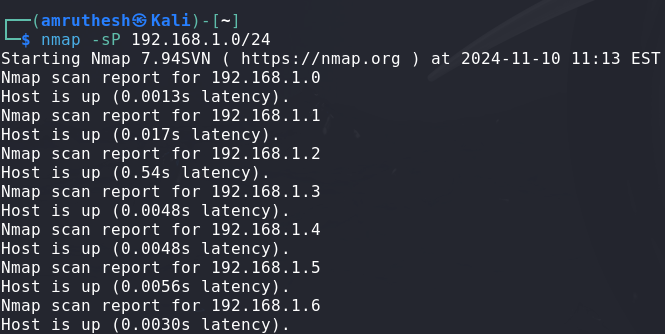
#!/bin/bash

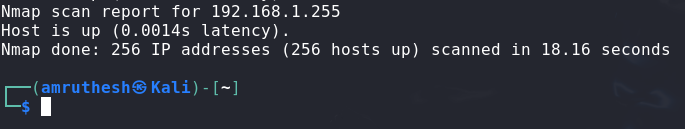
ifconfig | grep -E 'inet|netmask'



1. **Network Scan with Nmap**  
   To scan the local network:

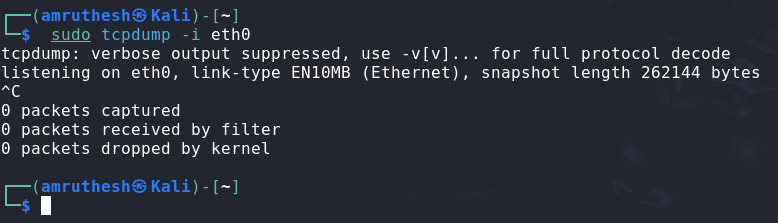
nmap -sP 192.168.1.0/24





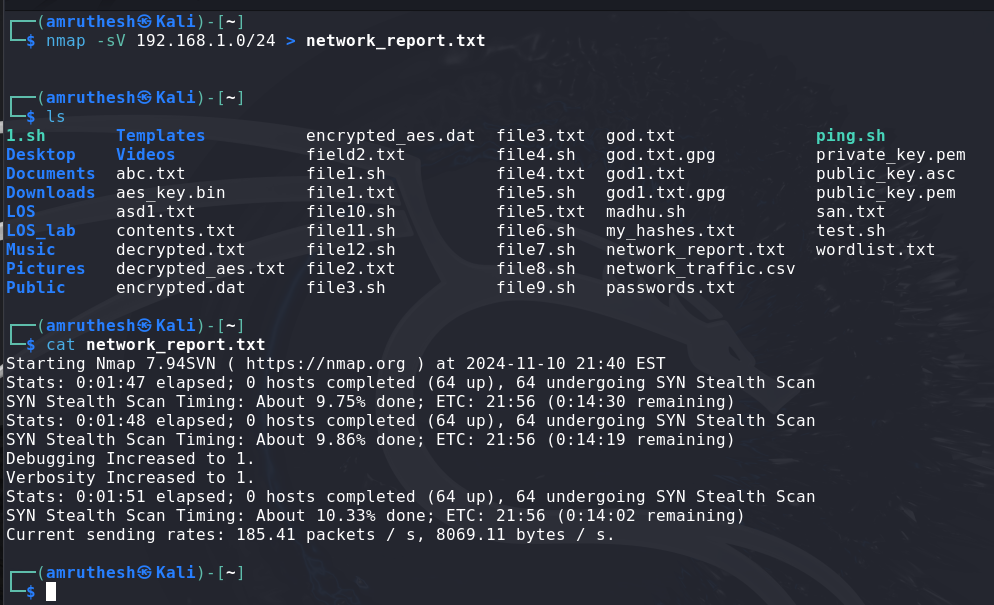
1. **Capture Network Packets with Tcpdump**  
    To capture packets on a specific interface (e.g., eth0):

sudo tcpdump -i eth0



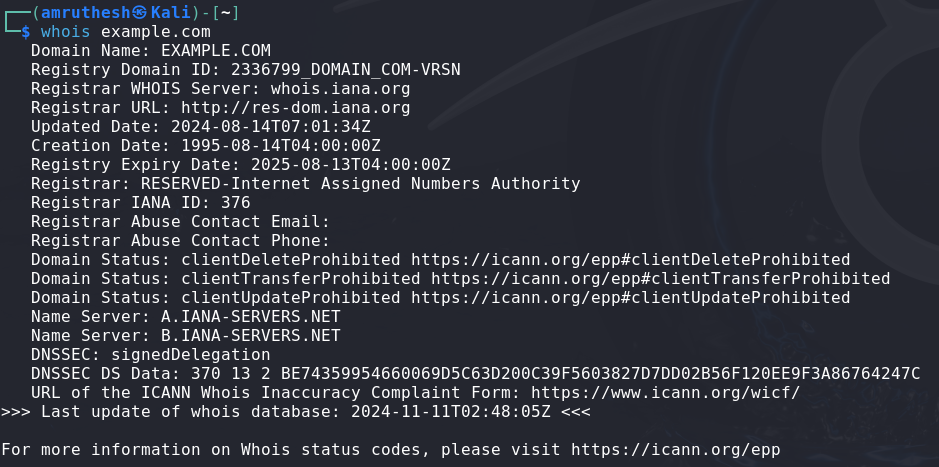
1. **Network Scan Report**  
   After running the nmap command, create a report with the IPs and services found:

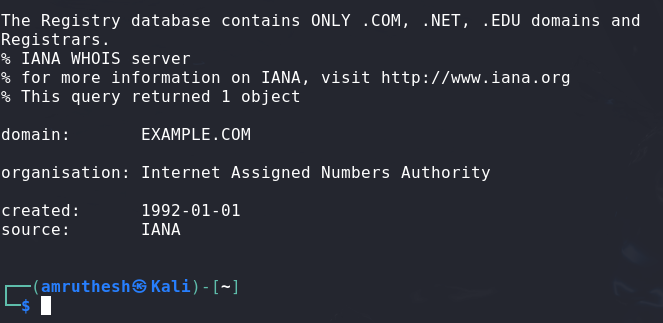
nmap -sV 192.168.1.0/24 > network\_report.txt



1. **Analyze Captured Packets for Specific Protocols**  
    Use the tcpdump output or tools like Wireshark to analyze protocols like HTTP or DNS.
2. **Whois Command**  
    To gather registration information about a domain:

whois example.com

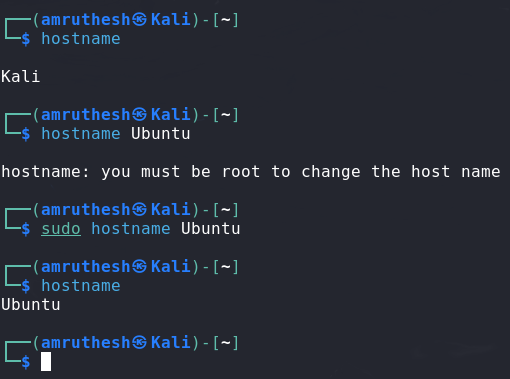


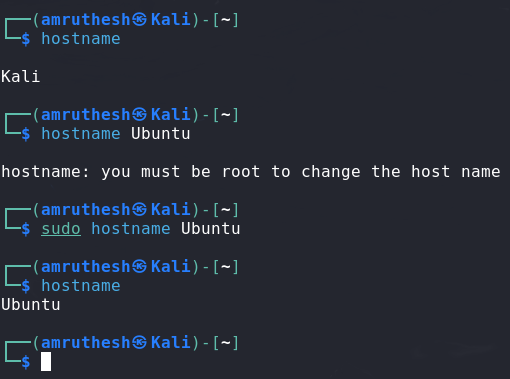


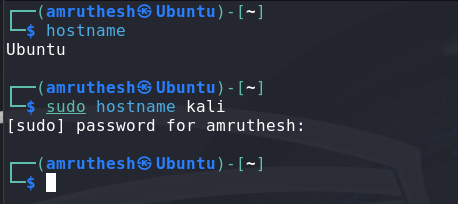
1. **Hostname Command**  
   To display and change the hostname of your machine:

hostname

hostname newname

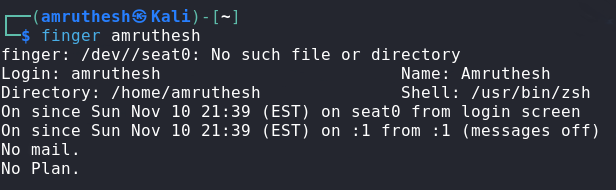






1. **Finger Command**  
   To gather information about users on a system:

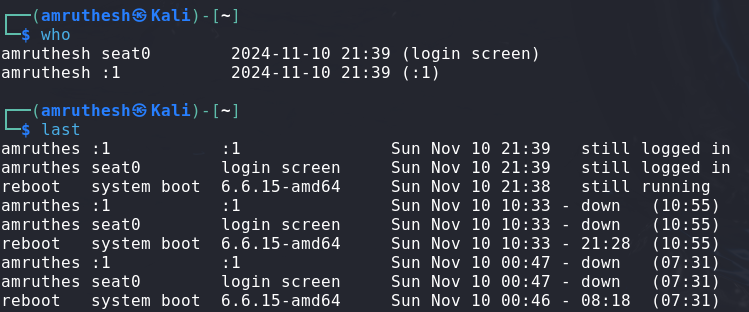
finger username

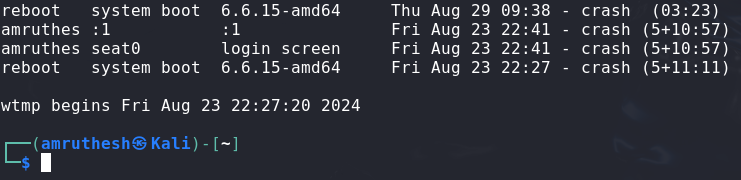


1. **Who and Last Command**  
   To see who is logged into the system and view login history:

who

last





**Xargs Tasks**

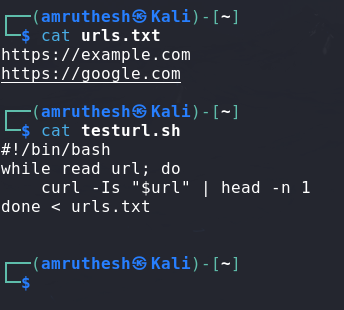
1. **Shell Script to Test URLs**  
   Script testurl.sh to check if websites are up:

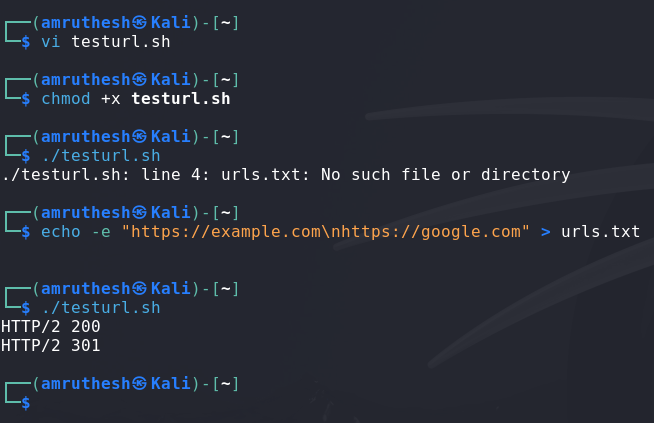
#!/bin/bash

while read url; do

curl -Is "$url" | head -n 1

done < urls.txt

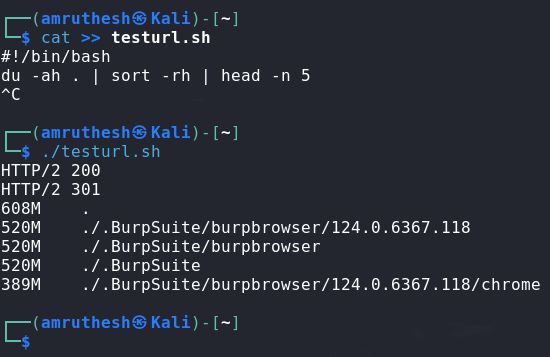




1. **Shell Script to List 5 Largest Items**  
   Script diskhog.sh to list the 5 largest items:

#!/bin/bash

du -ah . | sort -rh | head -n 5



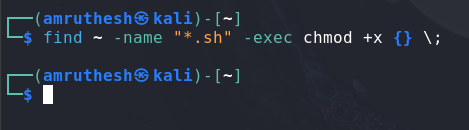
1. **Compress .log Files in /var/logs/**  
   Compress all .log files:

find /var/logs/ -name "\*.log" -exec gzip {} \;



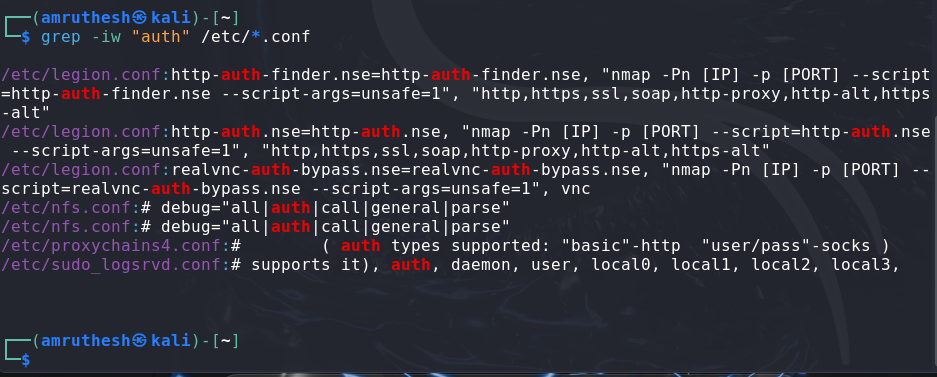
1. **Make All .sh Files Executable**  
   Make .sh files executable:

find ~ -name "\*.sh" -exec chmod +x {} \;



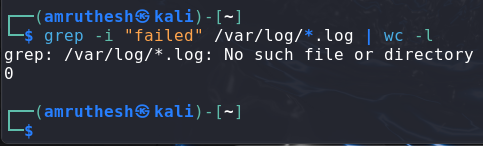
1. **Search for "auth" in .conf Files in /etc/**  
   Search for the string "auth":

grep -i "auth" /etc/\*.conf



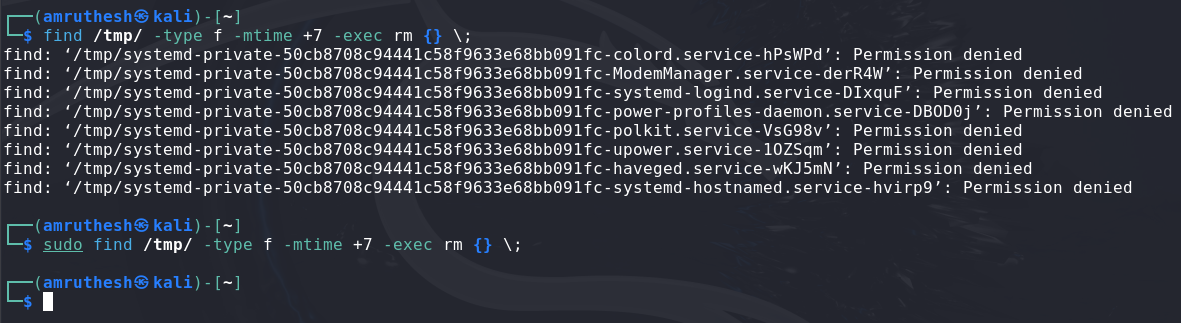
1. **Count Failed Login Attempts in .log Files**  
   Count failed login attempts:

grep -i "failed" /var/log/\*.log | wc -l



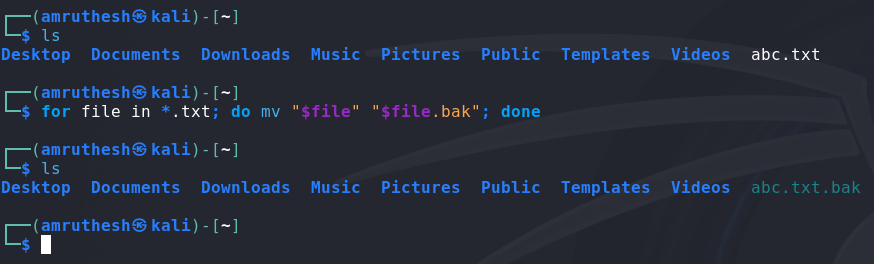
1. **Delete Temporary Files Older Than 7 Days**  
   Delete temporary files:

find /tmp/ -type f -mtime +7 -exec rm {} \;



1. **Rename .txt Files to Append .bak**  
   Rename .txt files:

for file in \*.txt; do mv "$file" "$file.bak"; done



1. **Check if Users Exist in the System**  
   Script to check if users exist:

#!/bin/bash

while read user; do

if id "$user" &>/dev/null; then

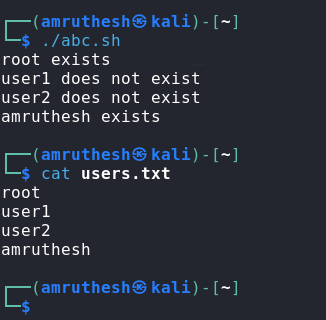
echo "$user exists"

else

echo "$user does not exist"

fi

done < users.txt



1. **Search for "ERROR" or "CRITICAL" in Log Files > 1MB**  
    Search in large log files:

find /var/log/ -size +1M -exec grep -i "ERROR\|CRITICAL" {} \;

