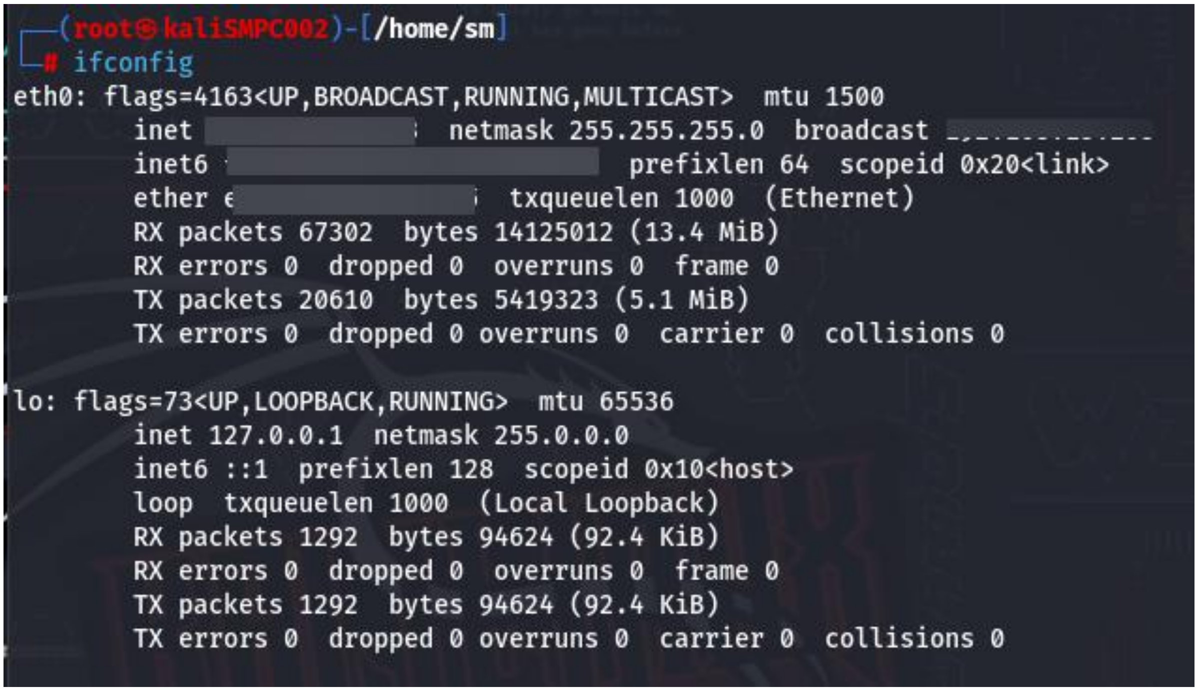
Linux Networking Commands

Linux offers a diverse array of networking commands to facilitate the management and troubleshooting of network configurations. Among the commonly used utilities is ifconfig, which provides essential details about network interfaces. For testing connectivity, the ping command is invaluable, while netstat offers comprehensive network statistics. These tools streamline network administration tasks and aid in the swift resolution of connectivity issues.

Commands such as route are essential for managing routing tables, ensuring efficient data transmission across networks. Additionally, iptables serves as a powerful tool for configuring firewalls, enhancing network security. With these commands at their disposal, Linux users can efficiently monitor and control network activity, troubleshoot connectivity problems, and fortify their systems against unauthorized access. The versatility and reliability of these networking commands make them indispensable for maintaining robust and secure network infrastructures in Linux environments, contributing to the overall stability and performance of the system.

Some Linux Networking Commands:

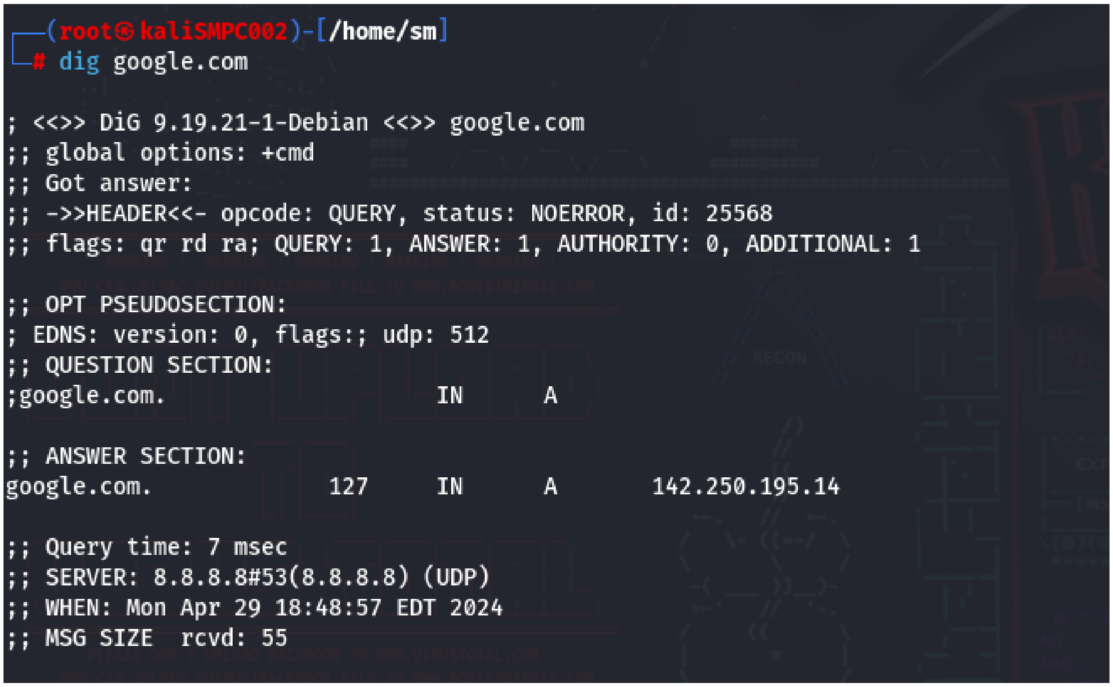
1.ifconfig is a command-line networking tool used in Linux systems to configure and display information about network interfaces. It provides details such as IP addresses, MAC addresses, network mask, broadcast addresses, and network statistics. With ifconfig, users can enable or disable network interfaces, assign IP addresses, set up routing, and troubleshoot network connectivity issues. While ifconfig has been widely used historically, newer Linux distributions may recommend using the "ip" command for network interface configuration and management, as it offers more features and flexibility. However, ifconfig remains a valuable tool for basic network configuration and monitoring tasks.



```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet [redacted]  netmask 255.255.255.0  broadcast [redacted]
        inet6 [redacted]  prefixlen 64  scopeid 0x20<link>
        ether [redacted]  txqueuelen 1000  (Ethernet)
        RX packets 67302  bytes 14125012 (13.4 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20610  bytes 5419323 (5.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1292  bytes 94624 (92.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1292  bytes 94624 (92.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

2. dig is a command-line tool used in Unix-like operating systems to perform DNS (Domain Name System) queries. It stands for "domain information groper". With dig, users can query DNS servers for various types of DNS records, such as A (IPv4 address), AAAA (IPv6 address), MX (mail exchange),

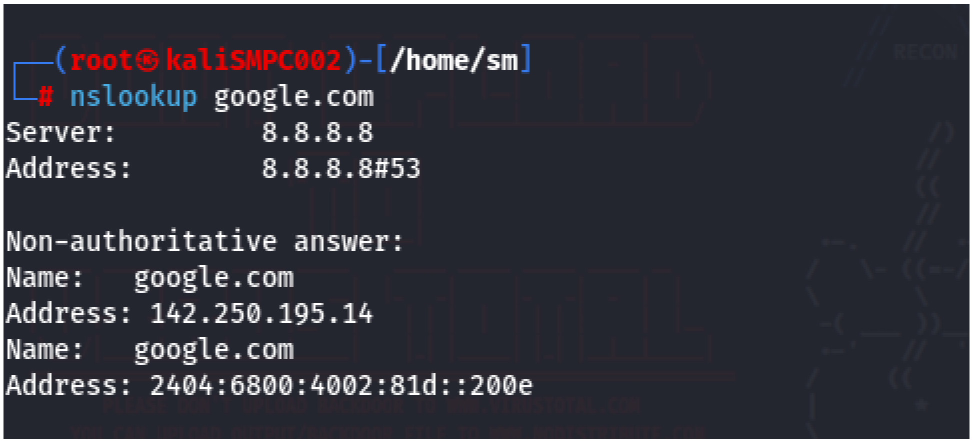
NS (name server), and more. It provides detailed information about the DNS resolution process, including the response time, authoritative DNS servers, and additional DNS records associated with the queried domain. Dig offers a flexible and powerful way to troubleshoot DNS-related issues, verify DNS configurations, and gather information about domain names and their associated DNS records.



```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# dig google.com

; <<>> DiG 9.19.21-1-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25568
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             127     IN      A       142.250.195.14

;; Query time: 7 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Mon Apr 29 18:48:57 EDT 2024
;; MSG SIZE  rcvd: 55
```

3. nslookup is a command-line tool used to query DNS (Domain Name System) servers to obtain domain name or IP address information. It stands for "name server lookup". With nslookup, users can perform various types of DNS queries, including forward and reverse lookups. In a forward lookup, users provide a domain name and nslookup returns its corresponding IP address. In a reverse lookup, users

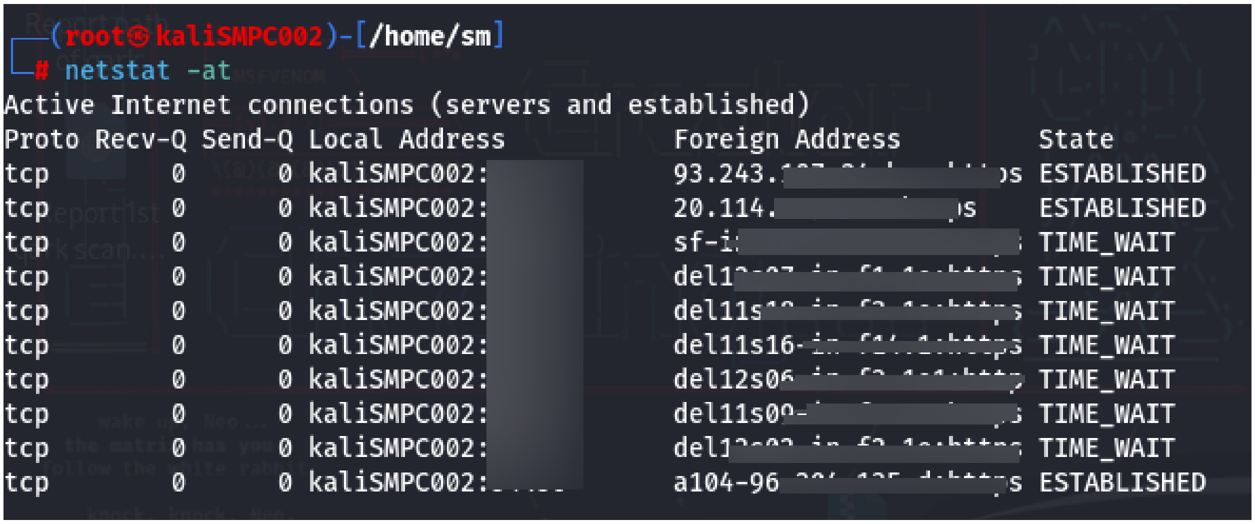
provide an IP address and nslookup returns its associated domain name. Additionally, nslookup can be used to query specific DNS record types such as A (IPv4 address), AAAA (IPv6 address), MX (mail exchange), NS (name server), and more. This tool is commonly used for troubleshooting network connectivity issues, verifying DNS configurations, and gathering information about domain names and their associated DNS records.



```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# nslookup google.com
Server:         8.8.8.8
Address:        8.8.8.8#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.195.14
Name:   google.com
Address: 2404:6800:4002:81d::200e
```

4. netstat is a command-line network utility tool available in Unix-like operating systems, including Linux. It displays various network-related information such as active network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. With netstat, users can monitor incoming and outgoing network connections, identify listening ports, view routing information, and track network traffic in real-time. It provides valuable insights into network activities, allowing users to troubleshoot network-related issues, identify network usage

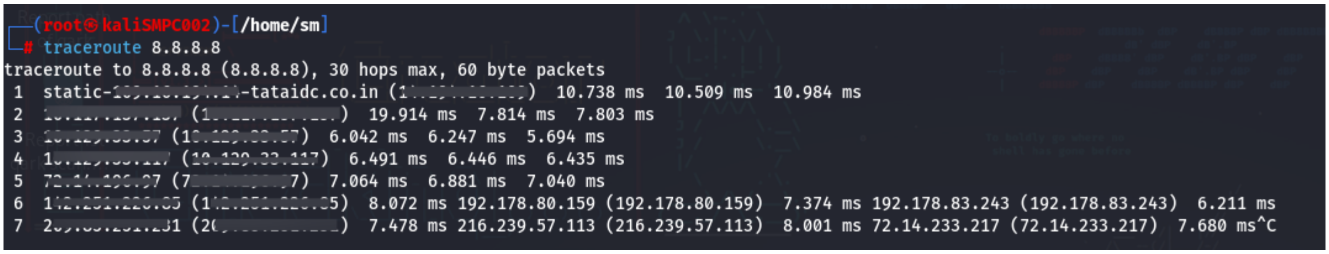
patterns, and diagnose network performance problems. Netstat is a versatile tool commonly used by system administrators, network engineers, and security professionals for network monitoring, analysis, and debugging purposes.



```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# netstat -at
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 kaliSMPC002:[redacted]  93.243.[redacted]ps     ESTABLISHED
tcp        0      0 kaliSMPC002:[redacted]  20.114.[redacted]s      ESTABLISHED
tcp        0      0 kaliSMPC002:[redacted]  sf-i[redacted]          TIME_WAIT
tcp        0      0 kaliSMPC002:[redacted]  del1[redacted]          TIME_WAIT
tcp        0      0 kaliSMPC002:[redacted]  del11s[redacted]        TIME_WAIT
tcp        0      0 kaliSMPC002:[redacted]  del11s16-[redacted]     TIME_WAIT
tcp        0      0 kaliSMPC002:[redacted]  del12s0[redacted]       TIME_WAIT
tcp        0      0 kaliSMPC002:[redacted]  del11s0[redacted]       TIME_WAIT
tcp        0      0 kaliSMPC002:[redacted]  del1[redacted]          TIME_WAIT
tcp        0      0 kaliSMPC002:[redacted]  a104-96[redacted]s      ESTABLISHED
```

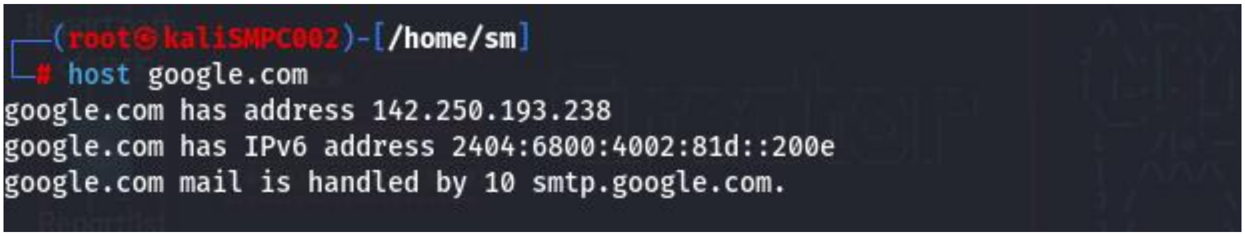
5. traceroute is a command-line networking utility used to trace the route that packets take from the local host to a specified destination host or IP address. It works by sending packets with incrementally increasing Time-to-Live (TTL) values and observing the ICMP Time Exceeded responses from intermediate routers. This process reveals the path packets follow through the network, showing each hop along the way. Traceroute provides valuable information about network latency and routing delays, helping users identify network congestion points, misconfigurations, and potential bottlenecks. It is commonly used for troubleshooting network connectivity issues, diagnosing routing problems,

and analyzing network performance. Traceroute is available on most Unix-like operating systems, including Linux, and it is an essential tool for network administrators, system administrators, and network engineers.



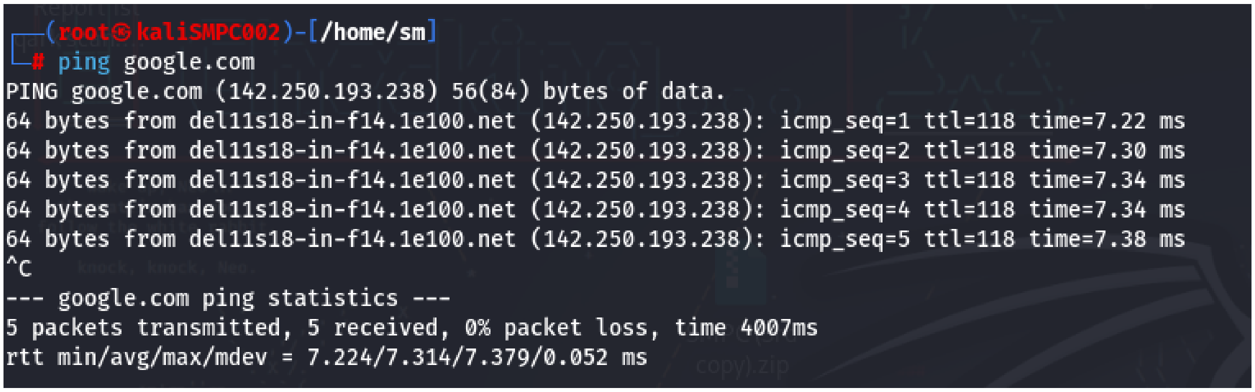
```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  static-[redacted]-tataidc.co.in ([redacted])  10.738 ms  10.509 ms  10.984 ms
 2  [redacted] ([redacted])  19.914 ms  7.814 ms  7.803 ms
 3  [redacted] ([redacted])  6.042 ms  6.247 ms  5.694 ms
 4  [redacted] ([redacted])  6.491 ms  6.446 ms  6.435 ms
 5  [redacted] ([redacted])  7.064 ms  6.881 ms  7.040 ms
 6  [redacted] ([redacted])  8.072 ms 192.178.80.159 (192.178.80.159)  7.374 ms 192.178.83.243 (192.178.83.243)  6.211 ms
 7  [redacted] ([redacted])  7.478 ms 216.239.57.113 (216.239.57.113)  8.001 ms 72.14.233.217 (72.14.233.217)  7.680 ms^C
```

6. host command is a versatile utility used for DNS (Domain Name System) lookups on Unix-like operating systems, including Linux. It performs DNS queries to retrieve various types of information related to domain names or IP addresses. When provided with a domain name, "host" returns the corresponding IP address(es) associated with that domain. Conversely, when given an IP address, it retrieves the corresponding domain name(s) if available. Additionally, "host" can query specific DNS record types such as A (IPv4 address), AAAA (IPv6 address), MX (mail exchange), NS (name server), and more. This tool is commonly used for troubleshooting network connectivity issues, verifying DNS configurations, and gathering information about domain names and their associated DNS records.



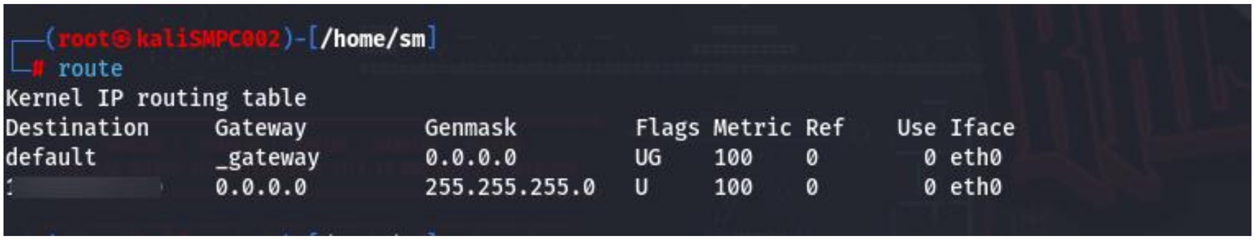
```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# host google.com
google.com has address 142.250.193.238
google.com has IPv6 address 2404:6800:4002:81d::200e
google.com mail is handled by 10 smtp.google.com.
```

7. ping command is a basic networking utility used to test the reachability of a host on an Internet Protocol (IP) network. It sends ICMP (Internet Control Message Protocol) echo request packets to the target host and waits for ICMP echo reply packets to come back. By measuring the round-trip time and packet loss rate, "ping" provides valuable information about network connectivity and latency. It's commonly used to diagnose network connectivity issues, verify network configurations, and assess network performance. The command is simple to use, typically requiring only the target hostname or IP address as an argument. For example, "ping google.com" sends ICMP packets to the Google website to check if it's reachable from the local system.



```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# ping google.com
PING google.com (142.250.193.238) 56(84) bytes of data.
64 bytes from del11s18-in-f14.1e100.net (142.250.193.238): icmp_seq=1 ttl=118 time=7.22 ms
64 bytes from del11s18-in-f14.1e100.net (142.250.193.238): icmp_seq=2 ttl=118 time=7.30 ms
64 bytes from del11s18-in-f14.1e100.net (142.250.193.238): icmp_seq=3 ttl=118 time=7.34 ms
64 bytes from del11s18-in-f14.1e100.net (142.250.193.238): icmp_seq=4 ttl=118 time=7.34 ms
64 bytes from del11s18-in-f14.1e100.net (142.250.193.238): icmp_seq=5 ttl=118 time=7.38 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 7.224/7.314/7.379/0.052 ms
```

8. route command is a networking utility used to view and manipulate the IP routing table in Unix-like operating systems, including Linux. It displays the current routing table, which contains information about how packets should be forwarded to their destination networks or hosts. Users can use the "route" command to add, delete, or modify routing entries in the table. Common tasks include adding static routes, changing the default gateway, and configuring specific routing policies. The "route" command is helpful for network administrators and system administrators to manage network traffic and troubleshoot routing issues. Additionally, it provides insights into how packets are routed through the network, aiding in network diagnostics and optimization.

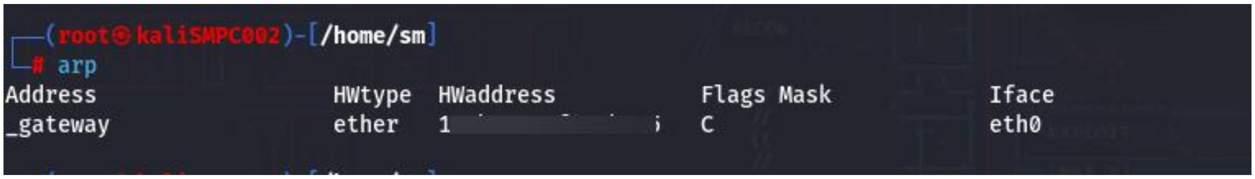


```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 eth0
[redacted]      0.0.0.0         255.255.255.0   U     100    0        0 eth0
```

9. arp command is a networking utility used to view and manipulate the ARP (Address Resolution Protocol) cache on Unix-like operating systems, including Linux. ARP is responsible for mapping IP addresses to MAC (Media Access Control) addresses on a local network segment. The ARP cache contains a list of IP addresses and their

corresponding MAC addresses, which helps devices communicate within the same network.

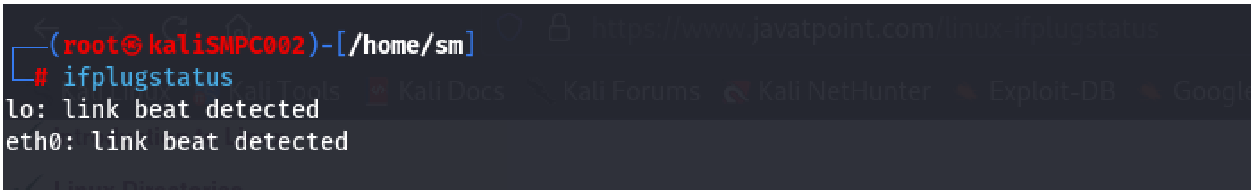
With the arp command, users can display the current contents of the ARP cache, add static ARP entries, delete ARP entries, and flush the entire ARP cache. This tool is commonly used for troubleshooting network connectivity issues, diagnosing ARP-related problems, and verifying the mapping between IP addresses and MAC addresses on a local network.



```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
_gateway                 ether   1[redacted]         C                     eth0
```

10. ifplugstatus command is a Linux utility used to check the status of Ethernet interfaces with respect to their link status. It is primarily used to determine whether a network cable is connected to a particular Ethernet interface or not.

When executed, ifplugstatus examines the link status of each Ethernet interface and reports back whether the interface is currently connected or disconnected. This information can be useful for network administrators and system administrators to quickly identify network connectivity issues, troubleshoot network problems, and ensure that network connections are properly established.



```
┌──(root㉿kaliSMPC002)-[/home/sm]
└─# ifplugstatus
lo: link beat detected
eth0: link beat detected
```