**Network commands**

**ping**

* Can be handful for DNS checks (up / or down) | is a DNS tool to resolves web addresses to an IP address.
* Test reachability - determine round-trip time, and uses ICMP protocol.

~#: ping www.google.com

PING www.google.com (172.217.168.164): 56 data bytes

64 bytes from 172.217.168.164: icmp\_seq=0 ttl=55 time=25.981 ms

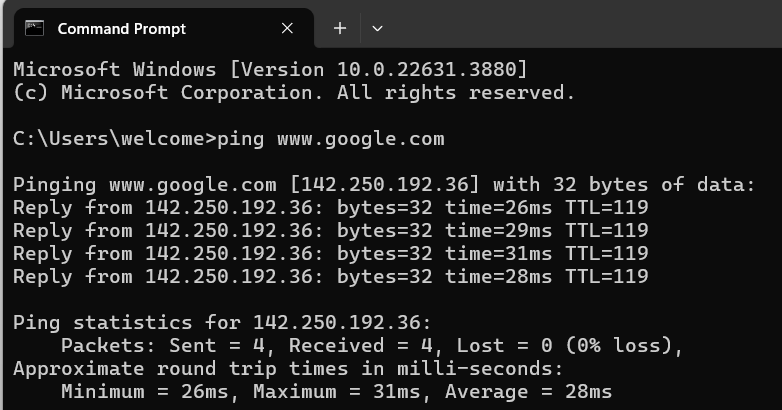
64 bytes from 172.217.168.164: icmp\_seq=1 ttl=55 time=25.236 ms

--- www.google.com ping statistics ---

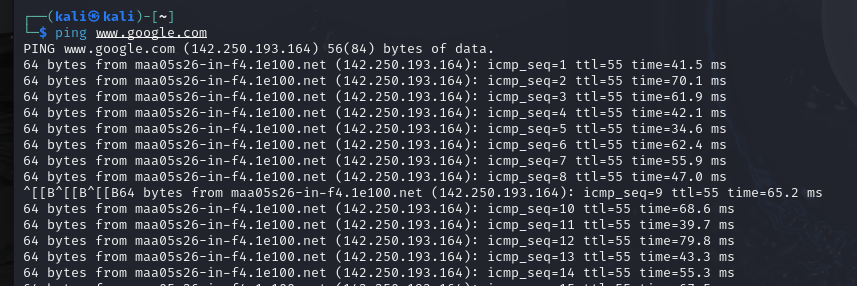
2 packets transmitted, 2 packets received, 0.0% packet loss

round-trip min/avg/max/stddev = 25.236/25.608/25.981/0.373 ms

**Windows –**

****

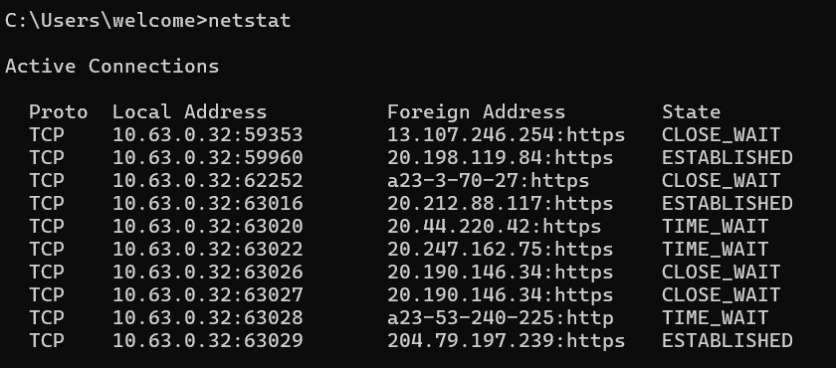
**Kali Linux –**

****

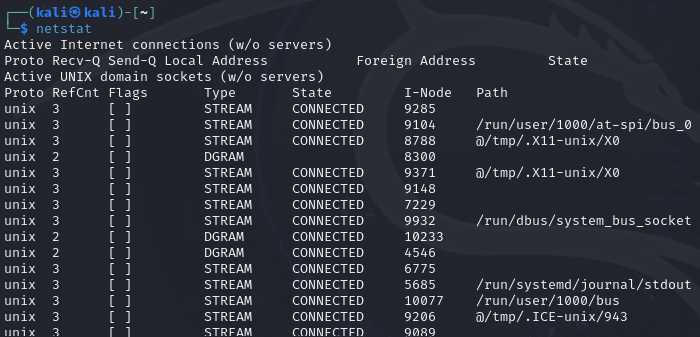
**Netstat**

* Network statistics
* Get info on host system TCP / UDP connections and status of all open and listening ports and routing table.
* Who you talking to?
* Who trying talking to you?

**Windows –**

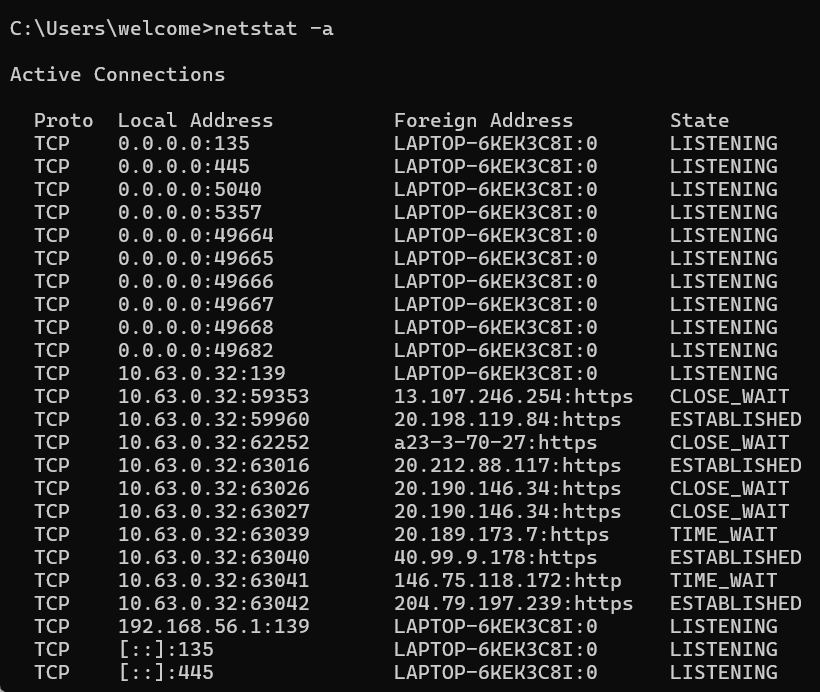


**Kali Linux -**

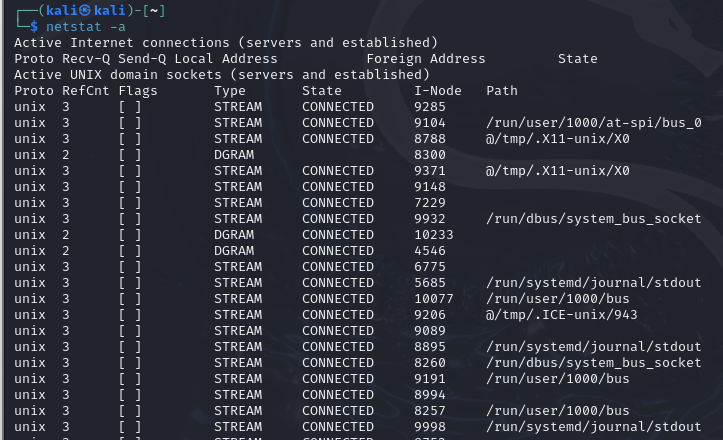


netstat -a # (show all active connections) (servers)

**Windows –**

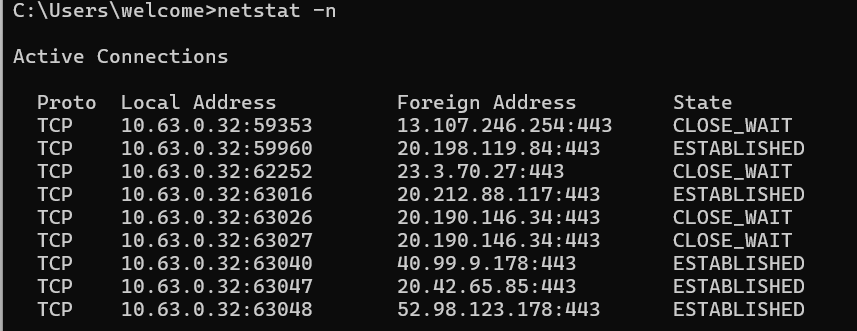


**Kali Linux -**

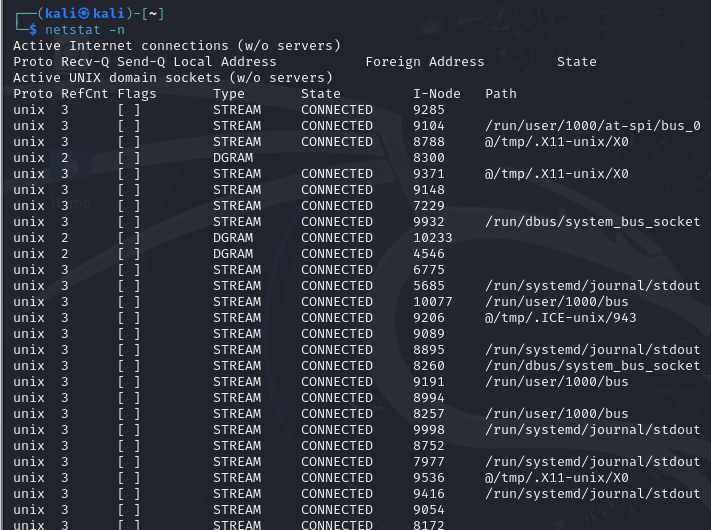


netstat -n # (hosts)

**Windows –**

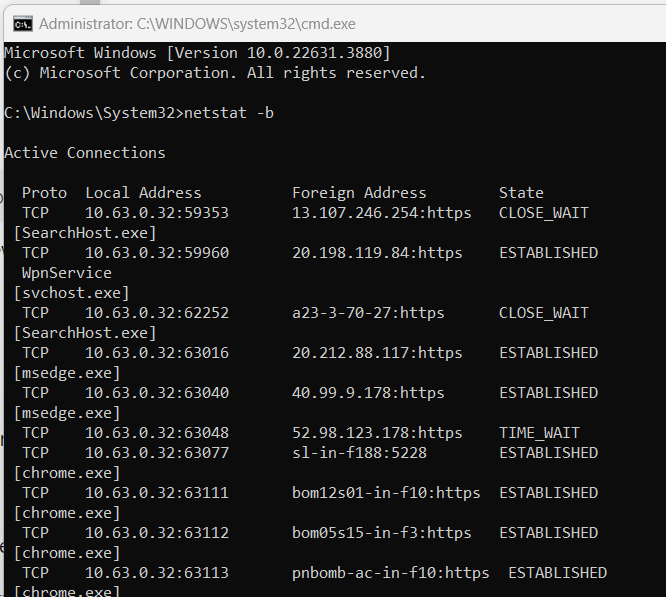


**Kali Linux -**



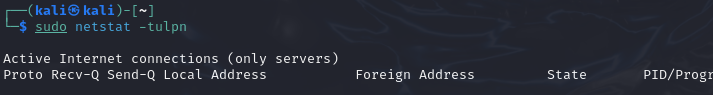
netstat -b # (Show binaries Windows)

**Windows –**



**Kali Linux -**

Equivalent command – sudo netstat –tulpn



**traceroute**

* Traceroute - how packets get from host to another endpoint. Traceroute is helpful to see what routers are being hit, both internal and external.
* **Take advantage of ICMP Time to Live (TTL) Exceeded error message**
  + The time in TTL refers to hops, not seconds or minutes.
  + TTL=1 is the first router.
  + TTL=2 is the second router, and so on.

~#: traceroute google.com

traceroute to google.com (172.217.17.14), 64 hops max, 52 byte packets

1 192.168.1.1 (192.168.1.1) 4.960 ms 3.928 ms 3.724 ms

2 10.10.124.254 (10.10.127.254) 11.175 ms 14.938 ms 15.257 ms

3 10.133.200.17 (10.137.201.17) 13.212 ms 12.581 ms 12.742 ms

4 10.255.44.86 (10.255.45.86) 16.369 ms 15.100 ms 17.488 ms

5 71.14.201.214 (71.14.201.214) 13.287 ms 29.262 ms 16.591 ms

6 79.125.235.68 (79.125.242.68) 22.488 ms

79.125.235.84 (79.125.242.84) 13.833 ms \*

7 79.125.252.202 (79.125.252.202) 24.147 ms

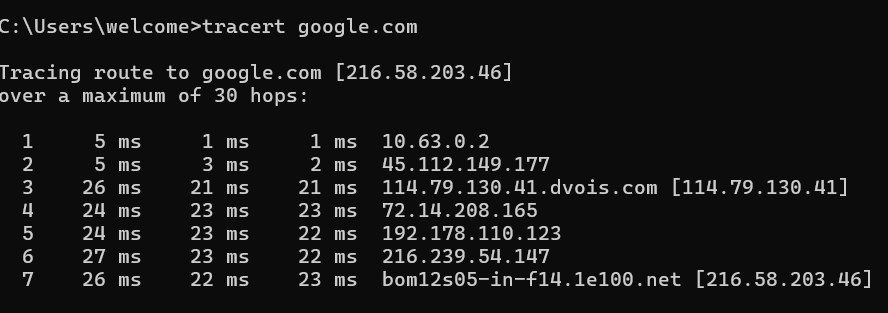
108.170.252.241 (108.170.25@.241) 26.352 ms

79.125.252.202 (79.125.252.202) 23.598 ms

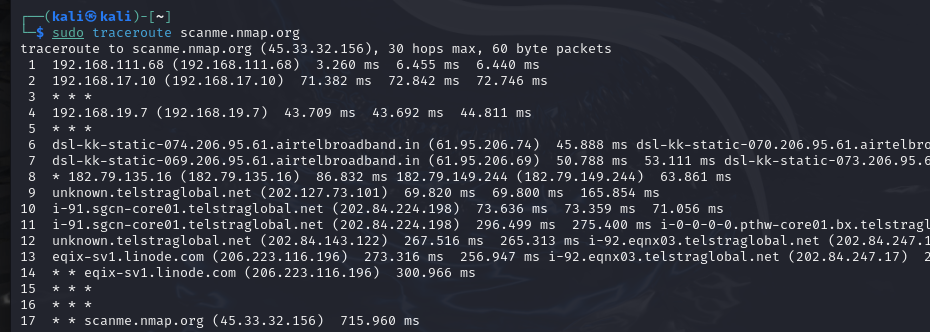
8 108.170.252.247 (108.170.252.247) 31.187 ms

79.125.252.199 (79.121.251.191) 22.885 ms

**Windows –**



**Kali Linux –**



**arp**

* Address resolution protocol - caches of ip-to-ethernet
* Determine a MAC address based on IP addresses
* Option -a: view local ARP table

~#: arp -a

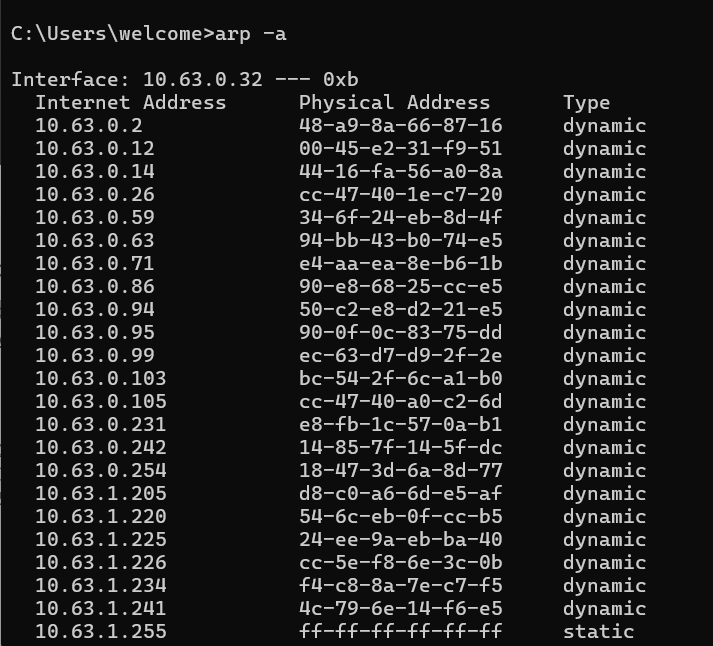
? (192.168.1.3) at 00:11:22:33:44:55 [ether] on enp0s10

? (192.168.1.128) at e8:33:b0:70:2c:71 [ether] on enp0s10

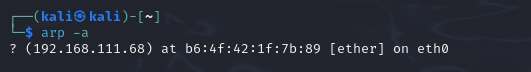
? (192.168.1.4) at 2c:33:5c:a4:2e:8a [ether] on enp0s10

\_gateway (192.168.1.1) at 00:31:33:8b:2a:da [ether] on enp0s10

**Windows –**



**Kali Linux –**



**ifconfig**

* Equivalent to ipconfig for UNIX/Linux OS.

~#: ifconfig

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500

ether 00:11:22:33:44:55 txqueuelen 0 (Ethernet)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s10: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.1.128 netmask 255.255.255.0 broadcast 192.168.1.255

inet6 fe80::acf6:2ae2:ab5c:6316 prefixlen 64 scopeid 0x20<link>

ether aa:bb:cc:dd:ee:ff txqueuelen 1000 (Ethernet)

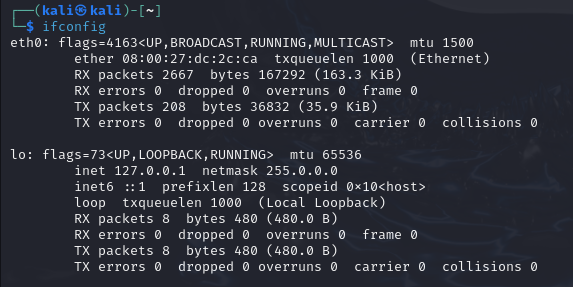
RX packets 156651 bytes 29382856 (28.0 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 76400 bytes 23111524 (22.0 MiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

**Kali Linux -**



**iwconfig**

similar to ifconfig, but is dedicated to the wireless network interface.

~#: iwconfig

lo no wireless extensions.

enp0s10 no wireless extensions.

wlp3s0b1 IEEE 802.11 ESSID:off/any

Mode:Managed Access Point: Not-Associated Tx-Power=19 dBm

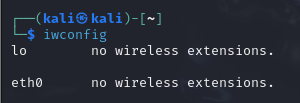
Retry short limit:7 RTS thr:off Fragment thr:off

Encryption key:off

Power Management:off

docker0 no wireless extensions.

**Kali Linux -**



**ip addr**

show / manipulate routing, network devices, interfaces and tunnels.

Show all the ip configuration, mac address, ipv6 etc.

~#: ip addr

1: lo: <LOOPBACK,UP,LOWER\_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000

link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

inet 127.0.0.1/8 scope host lo

valid\_lft forever preferred\_lft forever

inet6 ::1/128 scope host

valid\_lft forever preferred\_lft forever

2: enp0s10: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc fq\_codel state UP group default qlen 1000

link/ether aa:bb:cc:dd:ee:ff brd ff:ff:ff:ff:ff:ff

inet 192.168.1.111/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s10

valid\_lft 4761sec preferred\_lft 4761sec

inet6 fe80::acf6:2ae2:ab5c:6316 scope link noprefixroute

valid\_lft forever preferred\_lft forever

**Kali Linux -**



**nslookup**

* Query Internet name servers interactively; check if the DNS server is working

nslookup www.certifiedhacker.com

output:

Server: 192.168.1.1

Address: 192.168.1.1#53

Non-authoritative answer:

www.certifiedhacker.com canonical name = certifiedhacker.com.

Name: certifiedhacker.com

Address: 162.241.216.11 inslookup www.certifiedhacker.com

Server: 192.168.1.1

Address: 192.168.1.1#53

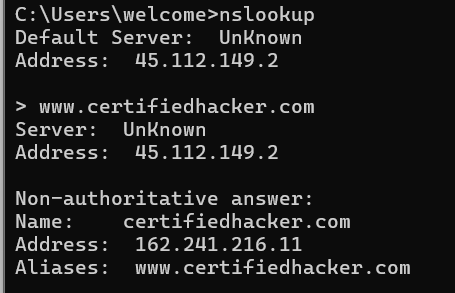
Non-authoritative answer:

www.certifiedhacker.com canonical name = certifiedhacker.com.

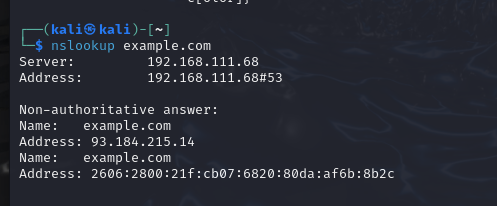
Name: certifiedhacker.com

Address: 162.241.216.11

**Windows –**



**Kali Linux -**



**dig**

* DNS lookup tool - Functions like nslookup, but allows for further functionality.

dig www.certifiedhacker.com

output:

; <<>> DiG 9.11.14-3-Debian <<>> certifiedhacker.com

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15708

;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 2048

; COOKIE: 71bd915b07b3fd08757c9ad65e5d6f3e549d5187359e97cb (good)

;; QUESTION SECTION:

;certifiedhacker.com. IN A

;; ANSWER SECTION:

certifiedhacker.com. 14400 IN A 162.241.216.11

;; Query time: 419 msec

;; SERVER: 192.168.1.1#53(192.168.1.1)

;; WHEN: Mon Mar 02 15:40:29 EST 2020

;; MSG SIZE rcvd: 92

**Kali Linux -**



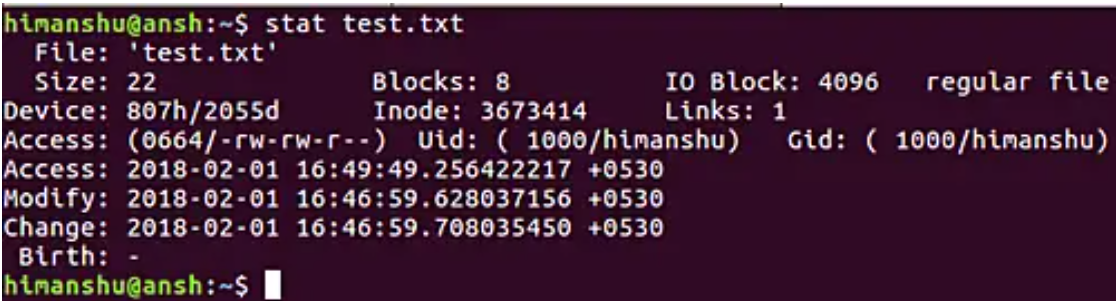
**netcat**

TCP/IP swiss army knife; you can make any type of connection and see the results from a command line. With nc you can connect to anything on any port number or you can make your system listen on a port number. Can be an agressive tool for recon.

* "Read" or "Write" to the network
  + Open a port and send or receive some traffic
  + Listen on a port number
  + Transfer data
  + Scan ports and send data to be a port
* Become a backdoor
  + Run a shell from a remote device

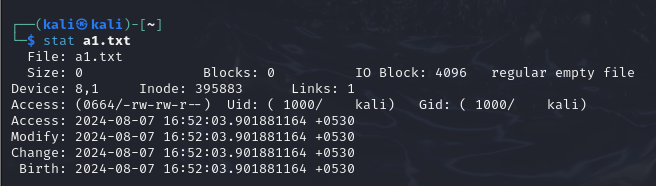
**stat**

stat can return the status of an entire file system, the status of the first hard disk and so on.



* Archive attribute - **Windows** - if something is created or changed

**Kali Linux -**



**tcpdump**

* Tcpdump is a data-network packet analyzer computer program that runs under a command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Distributed under the BSD license, tcpdump is free software

**Network Scanners**

**Useful for collect and inventory the hosts on a network, and is useful for reconnaissance of your system.**

**nmap**

The Best way to query a system to check if they have open ports, services, system versions, service versions etc.

nmap -v -A -T5 scanme.nmap.org

...

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)

| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)

| 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)

|\_ 256 33:fa:91:0f:e0:e1:7b:1f:6d:05:a2:b0:f1:54:41:56 (ED25519)

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

|\_http-favicon: Unknown favicon MD5: 156515DA3C0F7DC6B2493BD5CE43F795

| http-methods:

|\_ Supported Methods: GET HEAD POST OPTIONS

|\_http-server-header: Apache/2.4.7 (Ubuntu)

|\_http-title: Go ahead and ScanMe!

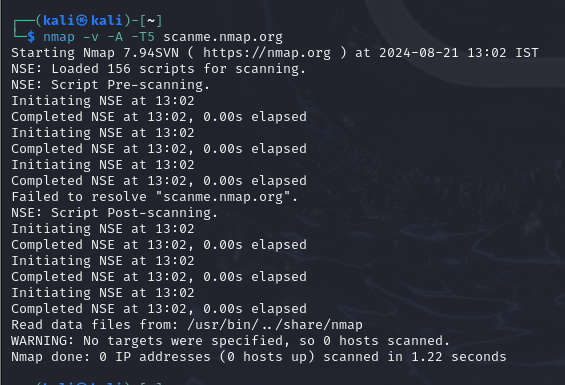
9929/tcp open nping-echo Nping echo

31337/tcp open tcpwrapped

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

...

**Kali Linux -**

S