**I – WHOIS EXERCISE**

**Pre-requirement: Install whois**

*(Ubuntu) #apt-get install whois*

*$whois coke*

Texto

Descrição gerada automaticamente

**Nmap tips**

**Understanding port states**

Nmap uses 6 different port states:

**Open**— An open port is one that is **actively accepting TCP, UDP or SCTP**[**connections**](https://nmap.org/book/man-port-scanning-basics.html). Open ports are what interests us the most because they are the ones that are vulnerable to attacks. Open ports also show the available services on a network.

**Closed**— A port that **receives and responds** to Nmap probe packets but there is **no application listening** on that port. Useful for identifying that the host exists and for OS detection.

**Filtered**— Nmap can’t determine whether the port is open because **packet filtering prevents its probes from reaching the port**. Filtering could come from firewalls or router rules. Often little information is given from filtered ports during scans as the filters can drop the probes without responding or respond with useless error messages e.g. destination unreachable.

**Unfiltered**— Port is accessible but Nmap doesn’t know if its open or closed. Only used in ACK scan which is used to map firewall rulesets. Other scan types can be used to identify whether the port is open.

**Open/filtered** — Nmap is unable to determine between open and filtered. This happens when an open port gives no response. No response could mean that the probe was dropped by a packet filter or any response is blocked.

**Closed/filtered** — Nmap is unable to determine whether port is closed or filtered. Only used in the IP ID idle scan.

**Nmap Basic exercise**

* https://phoenixnap.com/kb/nmap-command-linux-examples

**Nmap Advanced Tips**

<https://nmap.org/book/firewall-subversion.html>

**Firewall Evasion and Spoofing**

List of commands:

* -f or —- mtu = fragment packets and specify the fragment size as a multiple of 8. The idea of this is to split the packets into multiple smaller ones which makes the scan harder to detect and can be used to evade the IDS. Note: *Some programs have trouble handling fragmented packets.*
* -D = Decoy. This accepts a list of decoy hosts that will show to the target that you are scanning from. Note: that your IP address will be included amongst the list of decoys!! The position of your address among the decoys can be changed.
* -S = Spoof source address
* -e = Tell Nmap what interface to send/receive the packets from
* --source-port or -g = spoof source port number
* --data = Append custom binary data to packets (wonder what we can do with this 🤔)
* --data-string = Send a custom string along with the packet used as a comment e.g. “scan performed by system administrator”
* --data-length = Append random data to the packets to make the scan harder to detect
* --ip-options *<S|R [route]|L [route]|T|U ... >*; --ip-options *<hex string> =*Send packets with specified IP options. The options here allow you to record routes taken by packets and specify your [route](https://nmap.org/book/man-bypass-firewalls-ids.html).
* --ttl = Time to live for IPv4
* --randomize-hosts = Randomize target host order. Makes the scan less obvious
* --spoof-mac = Used to spoof the MAC address of the source. If you don’t specify all 12 characters then Nmap will randomly fill in the remaining ones.
* --proxies<comma seperated list of proxy urls in form proto://host:port = Relay TCP connections through a chain of proxies. Proxies are used to hide the source of the scan and to evade firewall rules.
* --badsum = Uses a malconfigured TCP/UDP checksum. This is used to probe the detection of a firewall or IDS. If a response is received then a firewall/IDS is present.