**active Reconnaissance**

1. **Introduction**
2. **Web Browser:**
3. **Ping:**
4. **Traceroute:**
5. **Telnet:**
6. **Netcat:**

* -l 🡪 Listen mode
* -p 🡪 Specify the Port number
* -n 🡪 Numeric only; no resolution of hostnames via DNS
* -v 🡪 Verbose output (optional, yet useful to discover an bugs)
* -vv 🡪 Very Verbose (optional)
* -k 🡪 Keep listening after client disconnects

1. **Putting It All Together:**

* ping 🡪 ping -c 10 10.10.82.94 on Linux or macOS

ping -n 10 10.10.82.94 on MS Windows

* traceroute 🡪 traceroute 10.10.82.94 on Linux or macOS
* tracert 🡪 tracert 10.10.82.94 on MS Windows
* telnet 🡪 telnet 10.10.82.94 PORT\_NUMBER
* netcat as client 🡪 nc 10.10.82.94 PORT\_NUMBER
* netcat as server 🡪 nc -lvnp PORT\_NUMBER