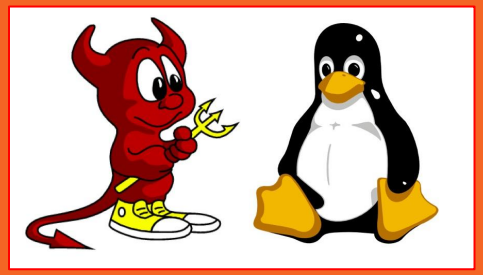

Unix/Linux
ISEN - AP4

T- TP nmap + sed ^^

2019 - J. Hochart

nmap

- Port scanner
- Essayer de se connecter à des hosts / services, avec plein de subtilités
- Sortir un rapport de “qui à répondu”

Options/usages classiques

- Targets
  - **Nmap 10.24.250.245:** Scan standard sur 1 IP
  - **Nmap 10.24.250.202-255:** Scan standard sur N IP
  - **Nmap sdf.lonestar.org:** Scan standard sur 1 host
  - **Nmap 10.24.250.0/24:** Scan sur un subnet

Options/usages classiques

- Ports
  - **Nmap -p 22 10.24.250.245:** 1 port
  - **Nmap -p 1-2048 sdf.lonestar.org:** Range de ports
  - **Nmap -F ...:** Fast (top 100)
  - **Nmap -p-:** 1-65535

Options/usages classiques

- Types de scan
  - **-sT: TCP connect:** Utilise le syscall connect()
  - **-sS: SYN scan:** Envoie des TCP Syn (default, fast)
  - **-sU:** UDP

Options/usages classiques

- Services
  - **-A:** OS + service fingerprinting
  - **-sV:** Service version detection

- Output
  - **-oN outfile:** Output standard dans un fichier
  - **-oG outfile:** Output grepable

Scan + output

- Se connecter à l’AP de TP
- Scanner un ensemble de cibles
  - Sur le réseau local
  - < 5 minutes: -F, peu de hosts en target
  - -sV
  - -oN nmap.txt

Sed

- Sur nmap.txt, utiliser sed pour “traduire le fichier en francais”
  - Example:
    - Nmap scan report for linuxbox (127.0.0.1)
      - → Rapport de scan pour linuxbox (127.0.0.1)
    - 22/tcp open ssh
      - → 22/tcp ouvert ssh
- Indenter (plus) les lignes contenant un port, et supprimer les lignes vides