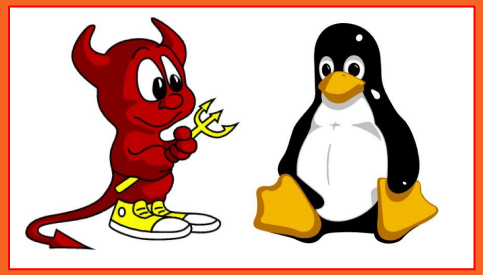
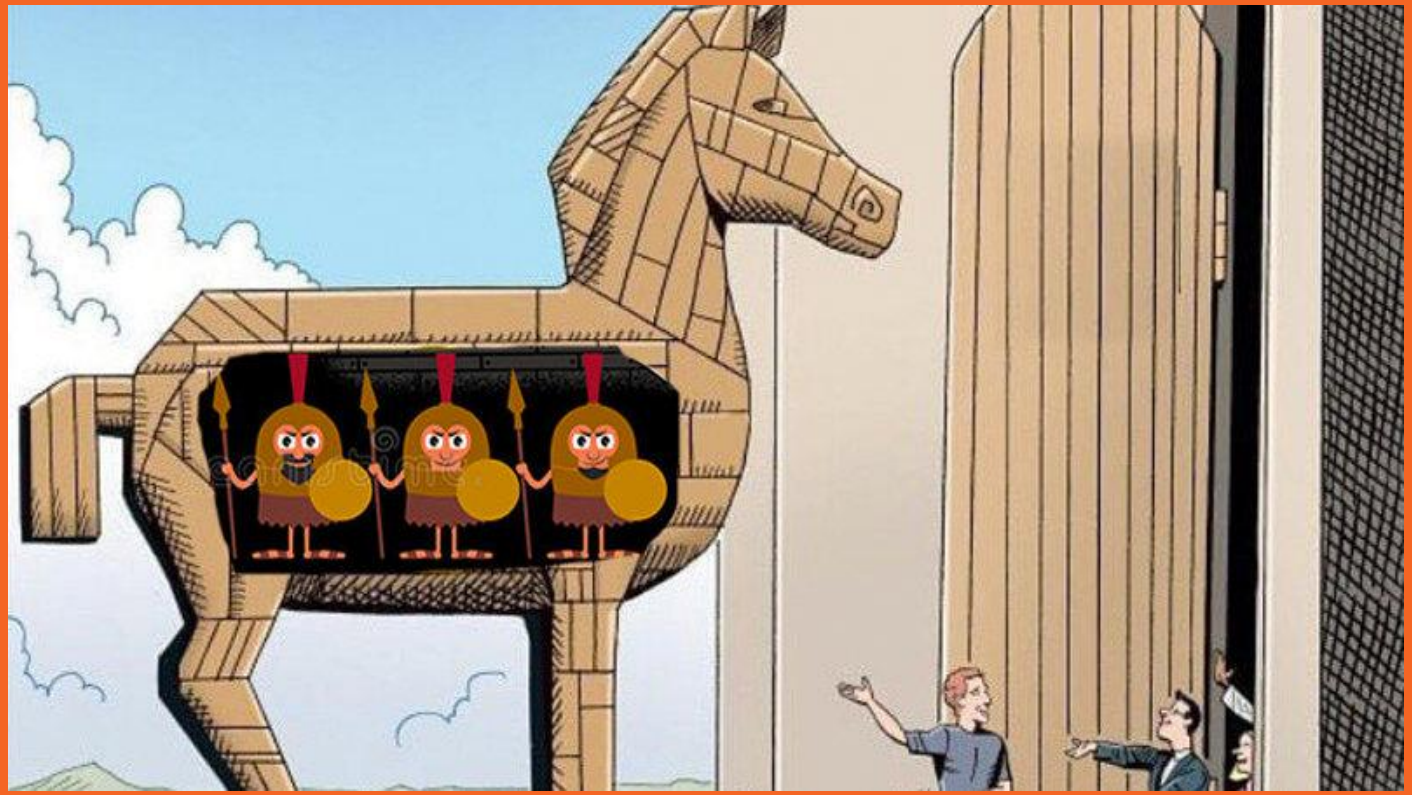


Unix/Linux
ISEN - AP4

Z- TP MyTrojan

2019 - J. Hochart

Trojan (horse)



Specs

- QQun laisse sa session ouverte en partant
- Quelles peuvent être les conséquences?
  - Compte user temporairement compromis
  - Maintien de l'accès
  - Trojan rudimentaire → netcat

Specs

- Le couteau suisse TCP/IP
- Comme telnet mais avec plus de fonctionnalités
- Client TCP
- Serveur TCP
- Proxy
- Port scanning
- Exécution de commandes
- ...

Specs

- Ecrire un 1-liner netcat trojan
  a. Ecoute sur TCP 6666 avec netcat
  b. Lecture de chaque message comme une commande à exécuter
  c. Exécution et log dans /tmp/trojan.log
  d. Lancement détaché avec nohup
  e. Retour en écoute dupliqué sur la socket au client

Exemple (côté client)

```
$ echo “whoami” | nc 10.0.0.2 6666
$ echo “reboot” | nc 10.0.0.2 6666
```

Specs

- Raccourcissement de la durée d’attaque
  a. Post du 1liner sur termbin
  b. Execution depuis termbin sur la machine victime (chrono)

Specs

- Adaptation pour osx