Notes de recherche-action sur l'administration système et l'administration réseau

Gestion

- Note n°1 : GhostScript et pdf

Sauvegarde

Défense

- Note 1 : Zip Bombe face à système invahissant

Réseau

Inspecter les connexion sur un réseau

- Note 1 : Quelques outils pour démarrer

Bypass Waf

IP addresses can be shortened by dropping the zeroes. Examples: http://1.0.0.1 → http://1.1 http://192.168.0.1 → http://192.168.1 This bypasses WAF filters for SSRF, open-redirect, etc where any IP as input gets blacklisted.

IPv4 is usually denoted as <octet>.<octet>.<octet>.<octet> (ff.0.1.2).

Can also be denoted as hex 0xff000102 or a number as in decimal notation. However, 4.2BSD's inet_aton() allowed IPs as decimal <octet>.<24bit-decimal> or <octet>.<octet>.<16bits-decimal>.

So the last “1” gets dereferenced as a decimal notation and is hence actually the two octets 0.1

For the same reason 1.1.257 gets resolved to 1.1.1.1 as 257 is actually 0x0101

Source witter /0xInfection/status/1148267196306427904

http://0xC0A80001 or http://3232235521 ⇒ 192.168.0.1. Works with ping and others too. sipcalc is your friend.

MyTraceRoute + Sysdig

https://www.libre-parcours.net/post/analyser-ses-communications-sur-internet-decouvrir-de-quels-reseaux-on-depend

Système

Ports

- Quels ports sont utilisés par quel processus sur une machine

```
$ sudo netstat -plnt | fgrep <port number>
```