Prova recuperació UF4 Seguretat

1.-(2,5pts) Implementa les regles Falco necessàries per tal de detectar els següents esdeveniments (el missatge a visualitzar en cada regla pot ser qualsevol). La resposta a l'exercici serà el contingut de l'**arxiu** "falco_rules.local.yaml" demanat i també un **vídeo** on es vegi l'execució de **cada** esdeveniment i l'aparició del missatge corresponent al Journal del sistema.

a) Cada lectura en el fitxer "/etc/passwd"

b) Cada execució de la comanda *ip*

2.-(2,5pts) Implementa, en una màquina virtual VirtualBox amb la seva tarja de xarxa en mode "adaptador pont", les regles Suricata necessàries per tal de detectar els següents esdeveniments. La resposta a l'exercici serà el contingut de l'**arxiu** "*.rules" demanat i també un **vídeo** on es vegi l'execució de **cada** esdeveniment i l'aparició del missatge corresponent al final de l'arxiu "fast.log"

a) Qualsevol petició TCP enviada des de la màquina real a la màquina virtual VirtualBox

b) Qualsevol resposta TCP enviada des de la màquina virtual VirtualBox a la màquina real

3.-(2,5pts) Realitza l'exercici nº5 de l'enunciat de l'"examen simulacre". La resposta a cada apartat d'aquest (n'hi han dos: a) i b)) haurà de ser un vídeo respectiu (és a dir, **dos vídeos** en total) demostrant que al mateix temps que es van fent peticions al servidor Apache2, efectivament es van recollint les dades a la gràfica en qüestió

4.-(2,5pts) Realitza l'exercici nº9 de l'enunciat de l'"examen simulacre". La resposta a l'exercici haurà de ser un **vídeo** mostrant com apareixen en temps real a la pàgina "Discover" del Dashboards missatges que contenen un camp, anomenat "comanda", el valor del qual són les comandes executades en qualsevol terminal de la màquina.