Prova final UF4 Seguretat

1.-(2pts) 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 escriptura en el fitxer "/etc/fstab"

b) Cada execució del programa *ping*

2.-(2pts) Implementa 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 HTTP enviada des de la màquina de treball dirigida als servidors "www.marca.es" o "www.hola.com"

b) Qualsevol paquet enviat des de la màquina de treball que inclogui la paraula "virus" en el seu contingut

3.-(2pts) Realitza l'exercici nº5 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.-(2pts) Realitza l'exercici nº9 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.

5.-(2pts) Realitza l'exercici nº10 de l'"examen simulacre". La resposta a l'exercici haurà de ser un **vídeo** mostrant com, al mateix temps que s'intenten fer inicis de sessió SSH a la màquina de treball des de qualsevol sistema (el propi local o algun de remot), l'histograma demanat que compta el nº total d'intents d'inicis de sessió (fallits o no) al llarg del temps classificats per IP d'origen va variant.