Examen recuperació UF3 i UF4 Seguretat

UF3:

1.-(4pts) a) Utilitza el paràmetre *-M* de *mitmdump* per aconseguir, després d'implementar l'atac "ARP-Spoofing", que quan una determinada màquina víctima atrapada per l'atac vulgui accedir a la web d'Arduino (https://www.arduino.cc), de forma automàtica vagi a parar sempre a la web del CIA (https://www.cia.gov) Entrega **un vídeo** on es vegi en plena acció l'efecte d'aquest atac i la comanda concreta *mitmdump* executada

b) Utilitza el paràmetre *--map-local* de *mitmdump* per aconseguir, després d'implementar l'atac "ARP-Spoofing", que quan una determinada màquina víctima atrapada per l'atac vulgui visitar qualsevol pàgina web, totes les fotos de tipus JPG (o millor dit, tots els recursos la URL dels quals acabi en ".jpg") d'aquesta pàgina siguin substituïts per l'arxiu "/usr/share/pixmaps/faces/puppy.jpg" local (pertanyent al paquet "gnome-control-center"). Entrega **un vídeo** on es vegi en plena acció l'efecte d'aquest atac visitant la pàgina https://elpais.com i la comanda concreta *mitmdump* executada

c) Utilitza el programa interactiu Mitmproxy (i empra els filtres adients si cal) per localitzar la petició concreta que envia en nom d'usuari i la contrasenya quan s'omple el formulari d'inici de sessió en el lloc web https://as.com Entrega **un vídeo** on es vegi en plena acció aquest robament de credencials.

2.-(3pts) Genera un "payload" Meterpreter executable Linux de tipus "HTTP reverse" per tal de, un cop implantat d'alguna manera -això no importa- en la màquina víctima, puguis connectar-t'hi amb ell via la teva consola Metasploit. Entrega **un vídeo** on es vegi tant la creació del "payload" com l'accés a la consola Meterpreter corresponent, un cop aquest "payload" es posa en marxa a la víctima

3.-(3pts) A partir d'un fitxer binari inicialment creat amb la comanda *sudo dd if=/dev/zero of=arxiu.exe bs=1 count=50*, i fent servir algun editor hexadecimal, edita el fitxer binari anterior per tal de què doni positiu si li apliquem un arxiu de regles ClamAV contenint la següent regla. Entrega **una captura** on es vegi el contingut hexadecimal i ASCII del fitxer generat (això ho pots aconseguir mitjançant comandes com *hexdump -C* o el propi *hexedit*) : *Manolita1;Target:0;(0|2)&(0|1);0,10:6d616d61::i;10,30:70617061::i;30,50:63616361::i*

UF4:

1.-(3pts) 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.-(3,5pts) 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

3.-(3,5pts) 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.