Examen UF3 Seguretat

1.-(3pts) 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 l'article de la Wikipedia: https://ca.wikipedia.org/wiki/Anarquisme, de forma automàtica vagi a parar sempre a la web del FBI (https://www.fbi.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/cat.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 paràmetre -B de *mitmdump* per aconseguir, després d'implementar l'atac "ARP-Spoofing", que quan una determinada màquina víctima atrapada per l'atac visiti qualsevol pàgina web, s'injecti, al final de la secció *<head>...</head>* del codi font d'aquesta pàgina visitada, el codi CSS necessari per ocultar tots els elements HTML de tipus * * Pista: això ho pots aconseguir jugant amb la propietat *display:;* consulta per exemple https://www.w3schools.com/cssref/pr_class_display.php per saber com funciona. Entrega **un vídeo** on es vegi en plena acció l'efecte d'aquest atac visitant la pàgina https://opensource.com i la comanda concreta *mitmdump* executada

d) 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://elpais.com Entrega **un vídeo** on es vegi en plena acció aquest robament de credencials.

2.-(2pts) a) Genera un "payload" Meterpreter basat en Python de tipus "TCP 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

b) Utilitza Meterpreter per "robar" els fitxers on es troben emmagatzemades les credencials que el navegador Firefox de la màquina víctima té guardades dels llocs webs que s'han anat visitant. Entrega **un vídeo** on es vegin les accions realitzades per aconseguir això

c) Desxifra les credencials anteriors per obtenir les contrasenyes i els usuaris d'aquests llocs webs. Entrega **un vídeo** on es vegin les accions realitzades per aconseguir això i les credencials obtingudes (tatxades, si vols)

3.-(2pts) a) 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:

Manolita1;Target:0;(0|1)&1;0,20:6d616d61::i;20,50:70617061::i

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*)

b) Instal·la el keylogger "logkeys" vist a classe a la teva carpeta personal (no cal que l'executis, però). Tot seguit, fes un escaneig amb *clam**d**scan* (no *clamscan*!) de tot el contingut de la teva carpeta personal per comprovar si ClamAV detecta (o no) la presència d'aquest keylogger. Entrega **un vídeo** mostrant d'una banda l'execució i resultat de l'escaneig, i de l'altra l'execució i resultat del keylogger (per demostrar que efectivament està instal·lat).

4.-(3pts) Registra't a https://tryhackme.com gratuïtament. Un cop hagis iniciat sessió, vés a "Learn"->"Search" i busca una màquina que s'anomeni "Basic Pentesting". Segueix tot el procés per finalment obtenir la "flag" que apareix escrita dins del fitxer "pass.bak" ubicat a la carpeta personal de l'usuari "k++" (els "+" oculten el caràcter real). Entrega el teu propi **document "walkthrough", amb captures de pantalla incloses**, de tot el procés que has hagut de seguir per finalment obtenir la "flag"