Examen recuperació UF2 i UF3 Seguretat

UF2:

1.-(3pts) Arrenca una màquina virtual VirtualBox amb la seva tarja de xarxa en mode "adaptador pont" i instal.la-hi el paquet "tor". Configura, a l'arxiu "/etc/tor/torrc", la seva directiva *SOCKSPort* per a què en lloc d´escoltar a la IP "loopback" escolti a la IP de la tarja de xarxa, i posa en marxa el dimoni. Tot seguit arrenca una segona màquina virtual també amb la tarja de xarxa en mode "adaptador pont" i instal.la-hi el paquet "torsocks". Configura aquest darrer programa per a què es connecti al servidor Tor remot que està funcionant a l´altra màquina virtual. Finalment executa-hi en aquesta segona màquina la comanda *curl https://check.torproject.org/api/ip* i tot seguit *torsocks curl https://check.torproject.org/api/ip* Entrega **una captura de cadascuna de les dues comandes *curl*** anteriors i una breu explicació, en **un document de text**, del resultat observat

2.-PREVI:(3,5pts) Arrenca una màquina virtual VirtualBox qualsevol amb la seva tarja de xarxa en mode "adaptador pont" i on, a més, hauràs d'iniciar un servidor Netcat escoltant al port 4444. Escriu en un fitxer les regles Nftables necessàries per tal d'aconseguir el següent (els apartats a) i b) són independents!).

a) Aconsegueix que només les peticions (i respostes) de tipus "ping" (és a dir, paquets ICMP tipus 8 i 0), DNS (és a dir, paquets UDP al/del port 53) i HTTP/S (és a dir, paquets TCP als/dels ports 80 i 443) funcionin però cap més tràfic pugui sortir ni entrar del/al sistema. Entrega **el fitxer de regles** pertinent

b) Aconsegueix que només s'hi pugui accedir al servidor Netcat des de la màquina real i cap altra. Entrega el fitxer de regles pertinent

3.-PREVI: (3,5pts) Arrenca una màquina virtual VirtualBox qualsevol amb la seva tarja de xarxa en mode adaptador pont i instal.la-hi (i habilita'l, per a que s'inicïi automàticament a cada reinici) un servidor SSH.

a) Implementa en la màquina virtual un servidor SOCKS a partir del servidor SSH i tot seguit implementa un túnnel des de la teva màquina real a aquest servidor SOCKS fent servir el client SSH de la teva màquina real. Finalment, configura el navegador de la teva màquina real per a què utilitzi aquest túnnel i vés a Internet. Entrega **captures** de les diferents comandes que has hagut d'executar tant en la màquina virtual com en el client per implementar aquest túnel, així com **una captura del navegador** on es mostri la seva barra de direccions juntament amb una pàgina web qualsevol d'Internet i, finalment, **una altra captura** mostrant la sortida de la comanda *ss -tn* tant a la teva màquina real com a la màquina virtual

b) Configura, tant el servidor SSH com el client SSH de la teva màquina real per a què implementin l'autenticació per claus per algun usuari concret de la màquina virtual. Entrega les **captures** de les diferents comandes que has hagut d'executar per aconseguir-ho.

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*