Prova Final UF2 Seguretat

PKI

1.-a) En una màquina virtual qualsevol, utilitza la comanda *step* per crear un certificat autosignat anomenat "ca.crt" (juntament amb una clau privada anomenada "ca,key") i tot seguit crear un certificat signat per "ca.key" anomenat "jajaja.crt" (juntament amb una clau privada anomenada "jajaja.key") vàlid per dos mesos i associat als noms DNS "jajaja.com" i "www.jajaja.com". Entrega **els fitxers ca.crt** i **jajaja.crt**

b) ¿Quina diferència hi ha entre afegir el paràmetre *-k*, o bé *--cacert* o bé *--ca-native* a una comanda *curl* quan es connecta a un servidor HTTPS? Entrega **un document de text** amb la resposta

TOR

2.-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

3.-Instal.la un servidor Apache2 a la mateixa màquina virtual on tens funcionant el servidor *tor* de l'exercici anterior i fes que només escolti a través de la IP loopback. Edita les directives adients de l'arxiu "/etc/tor/torrc" per a fer que el servidor Apache2 estigui disponible públicament al port 80 dins de la xarxa Tor com a servei "onion". Finalment, accedeix des de la màquina "client" amb el "Tor Browser" al domini ".onion" autogenerat del teu servidor web. Entrega **una captura** on es vegi el contingut del fitxer "/var/lib/tor/hidden_service/hostname" i **una altra captura** on es vegi la pàgina mostrada per l'Apache2 en accedir al domini ".onion".

VPN WIREGUARD

4.-Escriu un hipotètic arxiu "/etc/wireguard/wg0.conf" corresponent a un hipotètic servidor VPN per tal que l'adreça IP de la seva hipotètica tarja *wg0* sigui 10.0.0.1 i només tingui un "peer" reconegut (amb la IP 10.0.0.2/32). D'altra banda, escriu un altre hipotètic arxiu "/etc/wireguard/wg0.conf" corresponent a un hipotètic client VPN per tal que l'adreça IP de la seva hipotètica tarja *wg0* sigui 10.0.0.2 i només tingui un "peer" reconegut, que serà el servidor VPN anterior; has d'indicar també que vols que s'hi transmeti pel túnnel VPN tot el tràfic generat pel client, tingui el destí que tingui. Entrega **ambdós fitxers**

TALLAFOCS NFTABLES

5.-PREVI: 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

SSH

6.-PREVI: 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.

ALTRES TÚNELS

7.-Arrenca dues màquines virtuals qualssevol però que tinguin la seva respectiva tarja de xarxa en mode NAT (això és important!!) i instal·la el Global Socket Toolkit a cadascuna, si no ho tens ja. Executa:

a) Les comandes necessàries per poder executar remotament comandes (com si fos una sessió SSH entre una màquina i l'altra). Entrega **dues captures de pantalla** on es vegin les comandes demanades executades a cada extrem (i la seva corresponent sortida per pantalla)

b) Les comandes necessàries per poder enviar un fitxer d'una màquina a l'altra (com si haguéssim utilitzat *scp* o similar). Entrega **dues captures de pantalla** on es vegin les comandes demanades executades a cada extrem (i la seva corresponent sortida per pantalla)

EXTRA: DNS SEGUR

8.-PREVI1: Descarrega en una màquina virtual VirtualBox qualsevol amb la tarja de xarxa en mode adaptador pont, el paquet AdGuardHome adient i executa en un terminal el binari obtingut per tal d'accedir (remotament via web) a l'assistent inicial de configuració (tal com ja se t'indicarà a pantalla). Un cop dins de l'assistent, indica a totes les seves pantalles els valors que tu vulguis excepte a la primera, on has d'indicar que tant el servidor HTTP com el servidor DNS integrats en AdGuardHome escoltin en totes les adreces IPs (per aconseguir això últim hauràs d'aturar primer el servei "systemd-resolved" del teu sistema).

PREVI2: Arrenca una segona màquina virtual VirtualBox qualsevol (però que tingui entorn gràfic!) també amb la seva tarja de xarxa en mode adaptador pont i configura de forma temporal (amb la comanda *sudo resolvectl dns enp0s3 ip.primera.maq.virtual*) el servidor DNS que emprarà la teva tarja enp0s3 per a què aquest sigui el servidor AdGuardHome funcionant a la primera màquina virtual.

a) Vés a la pantalla inicial del panell web d'AdGuardHome. ¿Què indiquen les estadístiques "Top clients", "Top queried domains" i "Top blocked domains"? ¿Què vol dir el valor "Average processing time"? Entrega **un document de text** amb la resposta

b) Activa totes les llistes possibles de dominis sospitosos que AdGuardHome ofereixi a l'apartat "Filters"-> "DNS blocklists" i, de pas, actualitza-les. A partir d'aquí, obre el navegador de segona màquina virtual i visita des d'allà la pàgina "bepolite.eu". Mostra **una captura** de la pàgina obtinguda

c) Vés a l'apartat "Filters"-> "Custom filtering rules" de la configuració d'AdGuardHome i prohibeix la navegació al domini "oracle.com" (i tots els seus possibles subdominis). Fes-ho i comprova-ho des del navegador de segona màquina virtual. Mostra **una captura** de la pàgina obtinguda

d) Vés ara a l'apartat "Filters"-> "Blocked services" de la configuració d'AdGuardHome i bloca Instagram. Comprova que des del navegador de segona màquina virtual no pots navegar a "www.instagram.com". Mostra **una captura** de la pàgina obtinguda

e) Vés ara a l'apartat "Filters"-> "DNS rewrites" de la configuració d'AdGuardHome i fes que totes les peticions a "*.sport.es" es redirigeixin a "elpuig.xeill.net". Comprova què passa en intentar visitar des del navegador de segona màquina virtual la pàgina "www.sport.es" (o qualsevol subdomini relacionat). Mostra **una captura** de la pàgina obtinguda

Heu de triar 5 exercicis per fer, d'entre els 8 presentats. Cada exercici val 2 punts.
Totes les respostes les heu d'enviar adjuntes al correu q2dg2b@gmail.com