Prova final UF2 Planificació i administració de xarxes

HTTP

1.-(2 pts) a) Executa la comanda *curl* contra el servidor de Boredapi.com per mostrar al terminal només la descripció d'una activitat aleatòria que sigui per dues persones i de tipus "recreational" Envia **una captura de pantalla** on es vegi la comanda *curl* utilitzada a més del resultat obtingut

b) Executa les comandes combinades *eog, jq* i *curl* contra el servidor de Dog.ceo per visualitzar una imatge aleatòria d'un gos, el qual haurà de ser sempre de la raça (*breed*, en anglès) "chihuahua" . Envia **una captura de pantalla** on es vegi la combinació de comandes utilitzades, a més del resultat obtingut

c) Executa la comanda *curl* contra la URL única que t'hagi generat Webhook.site per enviar-hi via POST la següent dada JSON: *{'pepe':'1234','manolo':'5678'}* Envia **una captura de pantalla** on es vegi la comanda *curl* utilitzada a més de la dada JSON rebuda visible a la plana web de Webhook.site

d) Executa la comanda *curl* correcta per enviar un missatge (de tipus JSON o RAW, com vulguis) amb el tema que vulguis però amb el contingut "Venc Ford Fiesta" al servidor públic de Ntfy.sh. Tot seguit, en un altre terminal, executa la comanda *curl* correcta per anar mostrant tots els missatges que vagi publicant (cada cop que s'executi) el client emissor anterior. Envia **una captura de pantalla** on es vegin les dues comandes *curl* utilitzades a més del resultat obtingut en cadascun de les seves sortides.

DNS

2.-(2 pts) a) En una màquina virtual (Ubuntu o Fedora, tant se val) que tingui almenys una tarja de xarxa en mode "adaptador pont", afegeix al seu arxiu "/etc/hosts" una línia que associ la IP 5.6.7.8 amb el nom "*elteunom*.examen.com" (on "elteunom" ha de ser el teu nom). Tot seguit, modifica la configuració del seu servei "Systemd-resolved" per tal de què escolti peticions provinents de la xarxa i per a què pugui actuar com a servidor autoritatiu de la "zona" definida a l'arxiu "/etc/hosts" local. Executa a la màquina real la comanda *dig @ip.maq.virtual elteunom.examen.com* Envia **una captura de pantalla** on es vegi la comanda anterior i el seu resultat obtingut

b) Escriu un contingut realista d'un hipotètic arxiu anomenat "/etc/systemd/system/enp0s3.network", pertanyent a una hipotètica màquina de la mateixa xarxa que la màquina configurada a l'apartat anterior, on s'indiqui que la seva configuració de xarxa es vol que sigui dinàmica (és a dir, via DHCP) però que el servidor DNS desitjat es vol que sigui explícitament l'implementat a la màquina virtual anterior. Envia **una captura de pantalla** on es vegi el contingut d'aquest fitxer

WIRESHARK

3.-(2 pts) a) Obre amb el Wireshark el fitxer "exercici4.pcapng" penjat a la web del centre. Sabent que la informació que et mostra aquesta captura ha sigut generada per una conversa entre un navegador i un servidor HTTP, respon les següents preguntes **en un document**::

*¿Quina és la direcció MAC, la direcció IP i el port que utilitza el client i quina és la direcció MAC, direcció IP i port que utilitza el servidor?

*¿Quin és el significat del paquet que es mostra si s'escriu el filtre "*tcp.flags.syn==1 && tcp.flags.ack==0*"? ¿I si s'escriu el filtre "*tcp.flags.syn==1 && tcp.flags.ack==1*" ?

*Digues quin filtre de pantalla faries servir per veure només les peticions GET realitzades. A partir d'aquí, ¿quants i quins fitxers el navegador descarrega del servidor web en aquesta captura? ¿Quina opció del Wireshark hauries de fer servir per extreure aquests fitxers al teu disc dur?

*¿Quin és el nom per defecte del fitxer que el servidor web ofereix si rep la petició *http://192.168.75.1* ?

*Digues el número dels diferents paquets que realitzen la desconnexió TCP

b) Obre amb el Wireshark el fitxer "exercici5.pcapng" penjat a la web del centre. A diferència de la captura anterior, aquesta consisteix en una conversa entre un navegador i un servidor HTTP extern a la LAN del client Sabent això, respon les següents preguntes **en un document**::

*¿Per què totes les connexions amb IPs públiques tenen la mateixa MAC de destí? ¿Quina és la direcció IP de la màquina que té aquesta MAC? ¿Quina funció dedueixes que fa aquesta màquina?

*Escriu el filtre de pantalla "*http.request*" i sel.lecciona el paquet nº 117. Digues quin és el número de paquet que es correspon amb la seva resposta i com ho has esbrinat. Tot seguit, escriu el filtre de pantalla "*http.response*" i sel.lecciona el paquet nº125. Digues quin és el número de paquet que es correspon amb la seva petició corresponent i com ho has esbrinat.

*¿Quin és l'idioma que té configurat el navegador?

*¿Quins és el nom del diferent software servidor web que utilitzen els diversos servidors web contactats?

TSHARK

4.-(2pts) Digues una possible comanda de terminal concreta que hauries d'executar per tal de generar un tràfic de xarxa específic que es pogués mostrar a la sortida de cadascuna de les següents comandes Tshark. Envia **una captura de pantalla** per cada apartat on es vegi la comanda demanada adient

a) *tshark -Y "not arp" -T fields -e frame.time_epoch -e frame.protocols -e ip.src -e ip.dst -e udp.dstport -e _ws.col.Protocol*

b) *tshark -Y "dns and dns.flags.response == 1" -E header=y -T fields -e frame.time_epoch -e dns.qry.name -e dns.a*

c) *tshark -Y "http.request" -T fields -e frame.time_epoch -e ip.dst -e http.request.method -e http.request.uri -e http.user_agent*

d) *tshark -Y "http.response" -T fields -E separator=, -e http.response.code -e http.content_length -e text*

e) *tshark -Y "http or dns" -O http,dns*

OPENSEARCH

5.-(2 pts) A partir d'executar l'script *./tshark-os.sh "ip" "frame ip udp tcp icmp tls http dns ssh"* (vist a classe), implementa tot el necessari per aconseguir tenir els següents gràfics visibles en un panell Dashboards. Envia **una captura de pantalla** per cada apartat on es vegi la gràfica demanada:

a) Gràfic de línies, cadascuna corresponent a una resposta HTTP d'un determinat codi, on es compti el seu número al llarg del temps

b) "Pie chart" que compti la quantitat de paquets detectats classificats per port de destí i que s'autoactualitzi cada 5 s

c) "Pie chart" que compti la quantitat de paquets detectats classificats per IP d'origen i que s'autoactualitzi cada 5 s

Totes les respostes caldrà enviar-les adjuntes a l'adreça q2dg2b@gmail.com