Grau d'Enginyeria Informàtica: Gestió i Administració de Xarxes

Pràctica 6: escalat de serveis de xarxa, detecció de serveis i intrusions.

En aquesta pràctica realitzarem activitats de escalat de serveis de xarxa, monitorització i detecció de intrusions.

OBSERVACIÓ: algunes de les activitats relacionades amb el exercici 2 poden ser considerades com atacs o intrusions que poden tenir responsabilitats legals per tant es demana que aquesta activitat amb fins acadèmics solament es faci dintre de l'àmbit de pràctiques (NebulaCaos) proporcionat per l'assignatura i sobre estricta responsabilitat del alumne/a.

Exercici 1:

Fent servi la capacitat de Docker Swarm desenvolupar els següents apartats:

a) Analitzar les avantages de Docker Swarm (https://docs.docker.com/engine/swarm/), les principals ordres i instal·lar Docker sobre dues màquines connectades a la xarxa Internet.

Sobre una màquina configurar un cluster on una màquina sigui el manager i altre estigui com worker.

b) fent servir el següent Dockerfile crear en cada màquina una imatge (amb el mateix nom p.e. apache2-server) i que cadascuna desplegui un index.html diferent.

```
FROM ubuntu

RUN apt-get update
RUN apt-get -y install apache2
RUN echo "<html><body><h1>Executant: node X</h1></body></html>" > /var/www/html/
index.html

EXPOSE 80
CMD ["/usr/sbin/apachectl", "-D", "FOREGROUND"]
```

Reemplaçar la X per 1 o 2 per saber en quin node s'està executant la imatge. Verificar el seu funcionament.

c) Crear un service en el cluster amb dues instàncies, comprovar el seu funcionament, reduir a una instància i verificar que la xarxa Mesh funciona, comprovar el funcionament amb **ab** (paquet apache2-utils), escalar a 20 instàncies i tornar a fer servir el mateix test amb **ab** que per una instància. Extraure conclusions.

Exercici 2:

a) Instal·lar zenmap o nmapsi4 (GUI de Nmap) fer una anàlisis exhaustiu sobre B i C amb diferent profiles (intense, quick, regular, slow, amb TCP/UDP) analitzar el paràmetres i els opcions sobre Nmpap que comporten.

Grau d'Enginyeria Informàtica: Gestió i Administració de Xarxes

b) Repetir la instal·lació de **nmap** sobre D i analitzar el paràmetre -D o execucions com **nmap -P0 -sI 1.1.1.1:1234 10.10.10.x** (modificar X per la ip de A) que efecte tenen sobre A.

c) Fent servir iptables sobre les màquines *target* (A, B, C) fer un log dels *port scanning*. Instal·lar sobre aquestes el paquet **psad** analitzar els seu funcionament i detectar aquest *port scanning*. Analitzar amb aquest com es veu un *scanning* com la del punt b.

d) Analitzar el concepte de *honeypot* i defensa activa sobre una xarxa i crear un fent servir el paquet **labrea** (labrea.sourceforge.net/labrea-info.html) sobre D. Analitzar les seves funcions i deteccions. Utilitzar zenmap sobre A per generar connexions i el paquet **hydra o hydra-gtk** sobre A per intentar accedir a D. Analitzar des de D com es veuen aquests intents.

e) fent servir **prelude-lml** (https://www.prelude-siem.org/projects/prelude/wiki/PreludeLml) analitzar els logs de les diferents màquines sotmeses a *port-scanning/hydra*.

f) Analitzar i instal·lar sobre A el paquet **snort** i fer des de D diferents activitats de intrusions sobre A. Analitzar com aquestes queden registrades sobre A i com es fa snort para la seva detecció.

Generar un informe que inclogui les captura de pantalles més importants indicant com s'han resolt cadascun dels exercicis, indicar quins passos s'han seguit en la configuració, una descripció de cadascun i les verificacions realitzades de funcionament. Finalment afegir unes conclusions personals sobre la tasca desenvolupada explicant quines son les aportacions realitzades I inconvenients trobats.

L'informe s'haurà de lliurar al CV a les dates indicades (just abans de la següent sessió) i està sotmès a control de plagis.