Treball de Final de Grau Network Monitor

Cristina Nogués Freixas

1. Introducció

Aquest projecte consisteix en dissenyar i desenvolupar una aplicació d'administració de xarxes que permeti obtenir informació del seu estat. Aquesta aplicació està pensada per a que l'utilitzin els administradors de xarxa, per facilitar la seva tasca.

L'aplicació obté dades d'una xarxa mitjançant escanejos definits per l'usuari utilitzant, entre altres eines, nmap. Les dades que es recopilen són, ports, sistema operatiu, latència de les màquines, serveis, etc. Un cop finalitzat l'escaneig, es poden veure els resultats en forma d'informe. Els informes estan estructurats de manera que sigui fàcil i ràpid trobar les dades per a poder-ne treure conclusions. A més a més permet descarregar-los per a poder consultar-los en qualsevol moment sense necessitat d'estar connectat a Internet.

1.1 Objectius

A continuació, es descriuen els objectius en els quals esta basat aquest projecte:

- Obtenir informació útil de la xarxa (o equip) donat per l'usuari.
- Crear una eina de gestió de xarxes per a l'administrador.
- Crear una interfície web pràctica, intuïtiva i fàcil d'usar.
- Generar informes amb una estructura ordenada de les dades resultants al realitzar l'escaneig.
- Permetre la possibilitat de descarregar els informes.
- Tenir una aplicació minimalista, eficient i que es pugui utilitzar des de qualsevol dispositiu amb connexió a Internet.

2. Gestió del projecte

La gestió del projecte, s'ha dut a terme mitjançant paquets de treball i diagrames de PERT i GANTT que mostren en detall la distribució d'esforços de cada tasca, la relació entre els paquets de treball i els Milestones i Deliverables que s'han definit.

Els paquets de treball i tasques en els quals s'ha dividit el projecte, son els següents:

Paquet	Tasques
PT0 Gestió del Projecte	T0.1 Gestió de tasques T0.2 Gestió de recursos
PT1 Base de dades	T1.1 Disseny de la base de dades T1.2 Creació i implementació de la base de dades
PT2 Implementació de l'aplicació	T2.1 Disseny de la interfície T2.2 Desenvolupament del codi T2.3 Interacció amb la base de dades
PT3 Validació	T3.1 Control de funcionament
PT4 Documentació	T4.1 Estructuració de la memòria T4.2 Redacció de la memòria

Tabla 1: *Distribució dels paquets de treball*

3. Disseny

En aquest projecte, s'ha desenvolupat una aplicació web, encarada a administradors de xarxes, que permet obtenir dades d'una xarxa, com poden ser els ports oberts d'un cert rang de màquines, els serveis que hi ha actius, quines màquines hi ha actives, etc. Aquestes dades es recullen del programa nmap en un fitxer XML i posteriorment son tractades per a ser mostrades de manera més estructurada i visual per facilitar la seva lectura.

Les dades tractades del fitxer XML s'emmagatzemen a la base de dades i es mostren a la web en forma d'informe on es veuen ordenades i classificades, d'aquesta manera es més fàcil i ràpid trobar la informació que es percisa.

A l'informe les dades es classifiquen en tres parts:

- Informació general: És un resum de l'escaneig que s'ha realitzat. Conté les dades de l'escaneig en la seva versió reduida.
- Xarxa: Mostra un llistat amb detall de tots els equips actius a la xarxa.
- Serveis: Mosta un llistat amb detall de tots els serveis actius de la xarxa.

Totes les dades que es mostren a l'aplicació s'han extret majoritàriament de nmap, però també s'han utilitzat altres comandes de linux com: whois, dig, top, df, etc.

A l'hora de dissenyar la web, s'ha optat per un disseny senzill i minimalista per a fer més agradable la seva utilització i no atabalar a l'usuari. L'aplicació es fàcil d'utilitzar, compta amb un menú principal des del que es pot accedir a totes les seves funcionalitats.

El llenguatge de programació utilitzat ha estat PHP per la seva robustesa i bona integració amb MySQL, gestor de bases de dades que s'ha escollit per els mateixos motius.

Descripció de l'aplicació

L'aplicació té un menú principal des del qual es pot accedir a totes les funcions d'aquesta. A la pàgina principal (*Home*) hi ha informació relacionada amb el servidor on es troba instal·lada l'aplicació, també es mostra la ip de l'equip des del que s'està utilitzant i dades relacionades amb els informes.

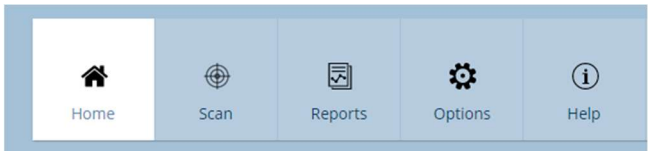

Ilustración 1: *Menú principal de l'aplicació*

Si s'accedeix a "*Scan*" es troba un formulari on l'usuari ha d'indicar el nom que li donarà a l'escaneig i la IP objectiu a escanejar, a continuació s'ha de triar un conjunt d'opcions predefinides que indiquen les dades que s'obtindran al realitzar l'escaneig. Aquests conjunts d'opcións es divideixen en quatre grups; simple, mitjà, pesat i personalitzat, on cada un d'ells contè les opcións del grup inmediatament inferior, es a dir, que el grup d'opcións del grup simple està contingut en el grup d'opcions del grup mitjà i aquest en el del grup pesat. D'aquesta manera podem obtenir mes o menys informació depenent de la necesitat. També hi ha el grup personalitzat que ofereix la posibilitat de triar només aquelles característiques que es vulguin. Per últim es dona la opció d'afegir arguments addicionals de la comanda nmap si es desitja.

Un cop iniciat l'escaneig, es pot veure a la pàgina principal (*Home*) el progrés d'aquest. Quan l'escaneig acaba, es crea un informe que es pot visualitzar accedint a "*Reports*" des del menú principal.

A "Reports" es troba el llistat amb tots els informes que s'han realitzat amb el nom de l'informe/escaneig, la data en la que s'ha realitzat i l'objectiu escanejat. Des d'aquí es poden visualitzar individualment cadascun dels informes, descarregar-los per tenir una copia o eliminar-los.

A l'apartat de les opcions, es pot canviar la contrasenya per accedir a l'aplicació i també els colors de la web per a millorar-ne la visualització. Hi ha dues alternatives d'estil de colors. Un en cas de que es terballi en un entorn amb molta llum i l'altre per a un entorn fosc.

Finalment, l'aplicació ofereix una ajuda on es fa una breu descripció d'aquesta i explica cadascún dels apartats de la web. A més a més també proporciona una llista de preguntes mes freqüents que ajuda a entendre millor el funcionament de l'aplicació.

3.1 Diagrama de casos d'us

El diagrama de casos d'ús és una tècnica per capturar els requisits potencials d'un nou sistema. Un cas d'ús és una seqüència d'interaccions que es durà a terme entre un sistema i els seus actors (usuaris) en resposta a un esdeveniment que inicia un actor principal sobre el propi sistema. El diagrama de casos d'ús serveix per especificar la relació entre els usuaris i els casos d'us d'un sistema. Una relació és una connexió entre els elements del model. Per tant, com es pot veure en el següent diagrama, en aquest cas, existeixen 7 casos d'us.

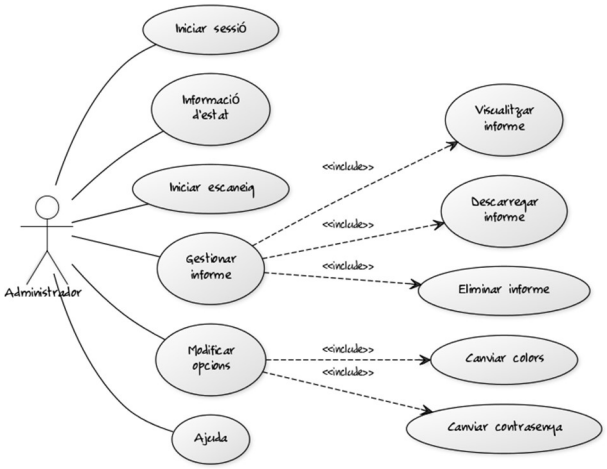

Ilustración 2: *Diagrama de casos d'us*

3.2 Diagrames de flux

Comportament de l'aplicació per fer un escaneig

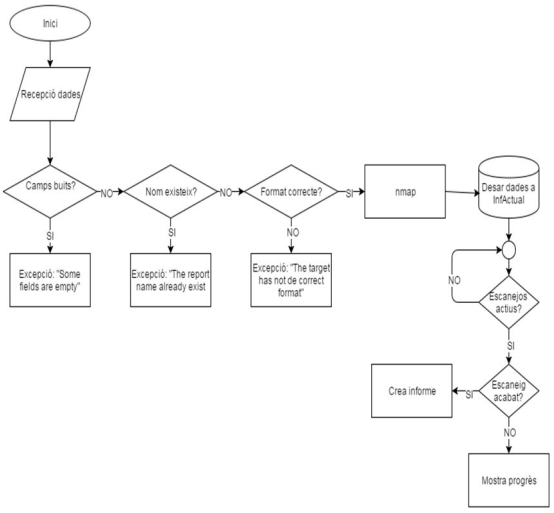

Ilustración 3: *Diagrama de flux del comportament per fer un escaneig*

Comportament de l'aplicació en crear un informe

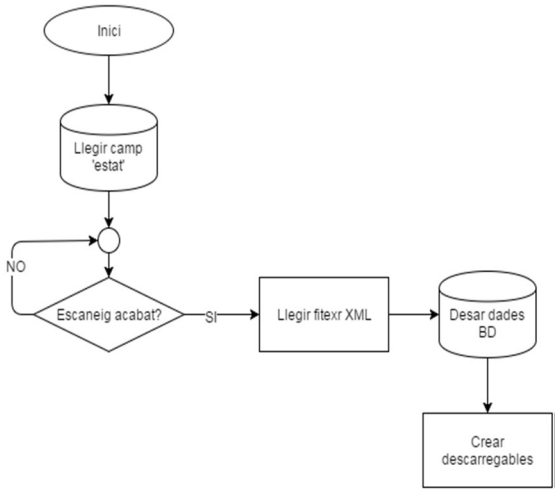

Ilustración 4: *Diagrama de flux del comportament al crear un informe*

3.4 Seguretat

La seguretat és un element bàsic per a qualsevol aplicació o servei. Les mesures de seguretat que s'han tingut en compte per a l'aplicació Network Monitor són, configurar HTTPS (*Hyper Text Transfer Protocol Secure*), per a una connexió segura a la web. SSH (*Secure Shell*) per a una connexió remota segura. Autenticació per a accedir a la web i Fail2Ban per a prevenir els accessos per força bruta. El tallafocs i copies de seguretat dels informes.

4. Tests i resultats

La màquina en la qual s'han realitzat els tests consta de les següents característiques:

- Màquina virtual amb el sistema operatiu Debian sense interfície gràfica.
- 8GB de disc dur.
- 500MB de memòria RAM

S'han fet diversos test d'estrès, manualment per una persona, per comprovar la capacitat que té l'aplicació en realitzar un nombre elevat d'escanejos al mateix temps.

Els escanejos del tipus "*Simple*" no tenen límit ja que acaben molt ràpid i no tenen temps d'acumular-se.

Per als escanejos del tipus "*Medium*" s'ha comprovat poden arribar a acumular-se fins a 15 aproximadament, es a partir d'aquest nombre, quan comencen a finalitzar els primers i per tant no arriben a acumular-se mes d'aquesta quantitat. Consumeix gairebé el límit de la memòria RAM.

Per als escanejos del tipus "*Hard*" s'ha comprovat que com a mínim es poden realitzar 20 escanejos a la vegada, però la web es comença a alentir ja que s'arriba al límit de memòria RAM.

En tots els casos l'ús de la CPU s'ha mantingut molt baix. Per tant a més memòria RAM més escanejos en el mateix temps es poden realitzar.

5. Conclusions i treball futur

5.1 Conclusions

S'ha aconseguit obtenir informació útil d'una xarxa o equip donats per l'usuari, mitjançant nmap, derivant la sortida d'aquest a un fitxer XML que posteriorment ha estat tractat per extreure les dades que finalment es mostren a l'informe. La part més complexa d'aquesta tasca ha estat tractar el fitxer XML ja que no ho havia fet mai i vaig haver d'investigar per saber-ho.

S'ha aconseguit crear una eina de gestió de xarxes per a un administrador de xarxes. *Network Monitor* compleix els requisits bàsics per a poder escanejar una xarxa o equip i treure conclusions de l'estat d'aquests.

S'ha aconseguit crear una interfície web senzilla i fàcil d'usar. La interfície és bastant minimalista però amb tot el necessari per poder realitzar la seva funció. En aquest aspecte s'ha creat un disseny senzill i s'ha intentat que sigui el mes estètic i agradable possible ja que no tinc coneixements en disseny web.

S'ha aconseguit generar informes amb una estructura ordenada de les dades resultants de realitzar l'escaneig d'una xarxa o equip. S'ha escollit la millor manera de presentar les dades per a una millor localització i enteniment d'aquestes, dividint-les en diferents pàgines i en

diferents blocs dins de cadascuna. A més a més s'ha aconseguit que aquests informes es puguin descarregar en format html, conservant així la funcionalitat dels enllaços. Aquesta part també ha tingut la seva investigació a l'hora de generar els fitxers de descarrega i fer que es puguin descarregar ja que no ho havia treballat mai.

S'ha aconseguit que l'aplicació sigui minimalista. S'ha usat el sistema operatiu Debian, sense interfície gràfica, en una màquina virtual de 8GB de capacitat d'emmagatzematge i 500 MB de RAM. A més a més al ser una aplicació web, s'aconsegueix que es pugui accedir des de qualsevol dispositiu amb connexió a internet.

5.2 Treball futur

En una continuació del projecte, una idea seria afegir la possibilitat de realitzar monitoritzacions de les xarxes de manera que a més a més de poder tenir informes de l'estat actual de la xarxa, poder conèixer els canvis d'aquesta al llarg del temps.

Es tractaria de fer dos tipus d'escaneig, un que recopili tota la informació (informe complet) i un altre que l'actualitzi (informe de manteniment). Es donaria la possibilitat d'escollir en quins intervals de temps realitzar els informes de manteniment.

També seria interesant tenir un "*log*" on anar veient els canvis i un sistema d'alarmes que avisés a l'usuari en casos d'amenaça.

6. Agraiments

Gràcies a totes les persones que s'han vist involucrades en el projecte d'una manera o altra, pel seu suport, la seva paciencia i la seva ajuda.

7. Referencies

[1] Flaticon Grapghic Resources. [en línia 31/05/2016] Disponible a: http://www.flaticon.com/

[2] The PHP Group. Documentació PHP [en línia 31/05/2016] Disponible a: http://php.net/manual/es/

[3] Stack Exchange. Stackoverflow fòrum [en línia 31/05/2016] Disponible a: http://stackoverflow.com/

[4] Oracle Corportaion. MySQL documentation [en línia 31/05/2016] Disponible a: http://dev.mysql.com/doc/

[5] Shapado 4.1.0 under GNU Aferro General Public License. AskDebian [en línia 31/05/2016] Disponible a: http://ask.debian.net/

[6] Fundación Wikimedia sota llicència Creative Commons. Wikipedia [en línia 31/05/2016] Disponible a: https://es.wikipedia.org/

[7] Das Plankton. Contrast-a-web V2.0 [en línia 31/05/2016] Disponible a: http://www.dasplankton.de/ContrastA/

[8] Standards OUI. MAC addresses [en linea 31/05/2016] Disponible a: http://standards-oui.ieee.org/oui.txt

[9] Refsnes Data. W3schools. HTML, CSS and Javascript Documentation. [en línia 31/05/2016] Disponible a: http://www.w3schools.com/

[10] Software in the Public Interest, Inc. Debian documentation. [en linea 31/05/2016] Disponible a: https://www.debian.org/doc/