Infraestructura i Tecnologia de Xarxes
Curs 2016-2017

Pràctica 5: *Scanners*

Introducció

Hi ha dos tipus principals d'escàners, els d'adreces IP i els de ports. Els escàners d'IPs es basen en fer *ping* a un rang de màquines per saber si aquestes estan enceses o apagades. Partint d'aquesta base, podem trobar eines més o menys avançades que incorporen algunes de les funcionalitats típiques dels escàners de ports o que permeten obtenir informacions tals com l'estat de NetBios [5], l'adreça MAC dels *hosts*, el grup de treball al que pertanyen, etc...

Per la seva banda, els escàners de ports són eines dedicades a comprovar si un *host* (habitualment un servidor) té alguns ports oberts i a obtenir informació sobre aquests. Aquests tipus d'eines són molt utilitzades des de dues vessants diferents:

- Els administradors de xarxes les utilitzen per verificar la seguretat i el compliment de les polítiques de seguretat. També les utilitzen per comprovar que els servidors ofereixen els serveis que s'espera d'ells, que els *firewalls* filtren els paquets que han de filtrar, etc...
- Els atacants utilitzen aquests tipus d'eines per obtenir informació sobre possibles objectius, esbrinar quins serveis corren a cada node, etc...

1 Eina utilitzada: Angry IP Scanner

Angry IP Scanner [4] és un Escàner d'IPs gratuït i multi-plataforma escrit en Java dissenyat per ser ràpid i fàcil d'utilitzar gràcies a la seva GUI. Disposa d'algunes funcionalitats addicionals i permet l'ús de *plugins* per cercar molts tipus d'informacions, exporta les dades obtingudes a diversos formats i realitza escaneigs de ports (com que ja els hem vist a la pràctica 6, no ens centrarem en aquesta funcionalitat).

El seu funcionament es basa en tres elements configurables:

- *Feeders* o generadors d'adreces a escanejar.
- *Fetchers*, determinen el tipus d'informació a obtenir per a cada *host* escanejat.

- *Openers*, serveixen per actuar de forma directa envers un node escanejat (establir una sessió SSH o TELNET, accedir al servidor web, etc...).

2 Eina utilitzada: Zenmap

Nmap [2] és un escàner de ports que va ser escrit originàriament per Linux amb l'objectiu de descobrir els *hosts* i els serveis en una xarxa, creant així un "mapa" d'aquesta. Actualment ha sigut portat a moltes altres plataformes i es distribueix de forma gratuïta. Per tant, és un dels escàners de ports més populars del món.

Nmap ha anat evolucionant i va molt més enllà de descobrir *hosts* i serveis, avui dia, s'adapta a les condicions de la xarxa (latència, congestió), detecta sistemes operatius i versions de *software* específic de servidors, té multitud de modes d'escaneig (pensats per esquivar mesures anti-escaneig o per evitar generar alertes en sistemes de detecció d'intrusions), permet guardar els resultats en diversitat de formats, etc...

Zenmap [3] és una interfície gràfica per a sistemes Linux. També és gratuïta i està pensada per facilitar l'ús de Nmap (s'encarrega de generar una comanda específica, amb tot un seguit d'opcions i paràmetres en funció de com configurem que volem que sigui la nostra cerca) i, sobretot, per a millorar l'extracció d'informació (navegació per menús, mapes visuals, possibilitat d'agrupar o filtrar serveis o *hosts*, etc...).

3 Guió de la pràctica: Sessió 1

Per executar Angry IP Scanner, obriu un terminal i executeu `ipscan`.

3.1 Escaneig de la xarxa del dEIC

1. **(0.25 punts)** Executeu un escaneig de tipus "IP Range" sobre el rang d'IPs `158.109.79.0` a la `158.109.79.255`. Trieu 3 màquines que estiguin enceses i no tinguin noms genèrics del tipus `deic-número.uab.es`.

IP:	Nom:
IP:	Nom:
IP:	Nom:

2. **(0.25 punts)** Aneu a "Preferences" (botó petit al costat de "IP Range") i modifiqueu les preferències de cerca per tal que Angry IP Scanner trobi algún node que no contesti pings, i algun node amb algun port obert que no sigui ni el 22 ni el 80. Torneu a executar la cerca anterior amb aquests nous

criteris. Llisteu un *host* que tingui obert algun port diferent del 22 i el 80, i algun node que no contesti pings.

A partir d'ara, podeu tornar a modificar les preferències de cerca com millor us vagi per tal de resoldre els següents exercicis.

3.2 Escaneig d'una altra xarxa

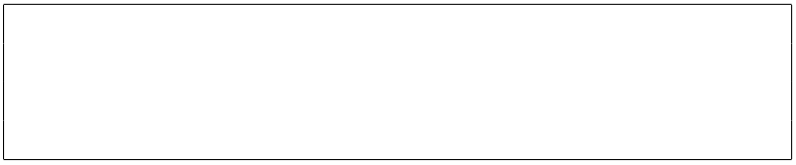
1. **(0.25 punts)** Executeu un escaneig de tipus "Random" sobre el rang d'IPs `158.109.79.0/16`. Identifiqueu quatre màquines de departaments/facultats diferents que estiguin enceses.

IP:	Nom:	Entitat:
IP:	Nom:	Entitat:
IP:	Nom:	Entitat:
IP:	Nom:	Entitat:

2. Executeu un escaneig de tipus "Random" sobre el rang d'IPs `158.109.X.Y/24` on els valors X i Y corresponen a una de les màquines que heu trobat al punt anterior.

3. **(0.75 punts)** Seleccioneu 4 *hosts* que tinguin obert el port 80. Utilitzeu "botó dret" $\rightarrow$ "Open" $\rightarrow$ "Web Browser" per obrir el navegador i intentar connectar-vos a aquestes màquines. Expliqueu a quin tipus de pàgines web us heu connectat (no s'admetran pàgines d'error o de login):

4. **(0.5 punts)** Ordeneu els resultats de la cerca per temps de resposta al *ping*. Els temps de resposta dels diferents nodes de la mateixa xarxa són similars o veieu algunes diferències significatives?



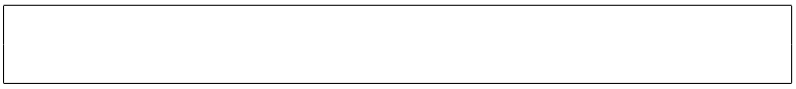
5. **(1 punt)** Trieu un *host* qualsevol d'aquesta xarxa i utilitzeu "botó dret" → "Open" → "Geo-locate" per obtenir les coordenades de la seva ubicació física. Compareu aquesta ubicació amb la que vosaltres suposeu que és la real. Coincideixen? Per què?

3.3 Una xarxa ja escanejada

L'altra dia l'Alícia va utilitzar Angry IP Scanner per tafanejar la xarxa del seu departament, però com que encara no ha cursat Infraestructura i Tecnologia de Xarxes, no va ser capaç d'interpretar els resultats del seu escaneig, per això els va exportar i pujar al campus virtual l'arxiu `scan.txt`, amb l'esperança de que algun alumne amb coneixements suficients tingués capacitat per resoldre els seus dubtes:

1. **(0.5 punts)** Des de que en Bob va canviar de despatx, des d'aleshores tots els dilluns i dimarts treballa de forma remota des de casa utilitzant SSH en comptes d'anar físicament a la universitat. Quin és el seu nou despatx? Com ho has sabut?

2. **(0.75 punts)** La setmana passada el Bob li va explicar que el nou becari del departament no en sap gaire de xarxes i que, tot i haver instal·lat un servidor web al seu ordinador, era incapaç d'accedir a ell des de casa. Sabries dir quina és la seva adreça IP? Com l'has trobat?



3. **(0.75 punts)** En Bob no té gaire clar si els dos estudiants de doctorat del despatx del costat s'han pres un any sabàtic o estan fent feina des de casa, ja que mai els veu al despatx. El que sí que sap és que tenen dues de les tres úniques màquines del departament que utilitzen Windows (l'altra és el servidor de noms). Saps com es diuen aquests estudiants? Atenen-te només a com van configurar les màquines, quin dels dos creus que realment està treballant des de casa i quin creus que pot estar de vacances al Carib?

4 Guió de la pràctica: Sessió 2

Habitualment, el tràfic que surt del laboratori de pràctiques està filtrat i no es poden realitzar escaneigs de ports de màquines situades fora d'aquest. Per a la realització d'aquesta pràctica, els dies 25/04/16 i 26/04/16, entre les 08:00 i les 15:00, eliminarem aquesta restricció i els podreu realitzar amb normalitat.

Per executar Zenmap, obriu un terminal i executeu `gksudo zenmap`.

NOTA: Fent "Explorar" → "Guardar todos los escaneos en un directorio" en qualsevol moment guardareu totes les dades que heu generat. Si no us dóna temps d'acabar la pràctica al laboratori, en qualsevol altre moment podreu utilitzar Zenmap per carregar les dades obtingudes en aquests escaneigs i acabar de resoldre les preguntes que us faltin.

1. **(0.5 punts)** Executeu un escaneig de tipus "intense scan" contra `venezia.uab.cat`. Quins ports té oberts? De què creieu que és servidor?

2. **(0.5 punts)** Executeu un escaneig de tipus "intense scan" contra `wiki.uab.cat`. Quan acabi, a la pestanya superior seleccioneu "Puertos/anfitriones" i a la columna de l'esquerra seleccioneu `wiki.uab.cat` com a "Anfitrión". Veureu que hi ha dos ports diferents oberts catalogats com HTTP. Per què?

3. **(0.5 punts)** Executeu un escaneig de tipus "intense scan" contra `www.uab.cat`. Quan acabi, analitzeu la "Salida nmap" i digueu amb quin sistema operatiu funciona `www.uab.cat`. Esteu segurs d'aquesta resposta? És exacta o aproximada?

4. **(0.5 punts)** Realitzeu un escaneig de tipus "quick scan plus" contra `158.109.79.67/29`. Analitzeu la sortida i trobeu quin és el servidor de noms dels equips del laboratori. Com l'heu trobat?

Resposta i justificació:

5. **(0.5 punts)** Utilitzeu la pestanya "Salida nmap" per analitzar els resultats produïts per els diferents escaneigs que heu executat. Digueu quines de les següents eines s'han executat durant l'escaneig.

☐ nast	☐ traceroute	☐ ping	☐ who	☐ ssh
☐ host	☐ iptables	☐ nmap	☐ accés a robots.txt	

6. **(0.5 punts)** Utilitzeu la pestanya "Topologia" per consultar el mapa de la xarxa. Amb quina informació Zenmap ha generat aquest mapa? Quines limitacions té aquest sistema?

7. **(0.5 punts)** Executeu un escaneig de tipus "regular" contra `wiki.uab.cat`. Utilitzeu l'eina "Comparar resultados" de Zenmap per comparar els resultats d'aquest escaneig amb el que heu realitzat al punt 2. Quines diferències trobeu?

8. **(1 punt)** Si examineu la informació que heu obtingut al realitzar els "intense scan", trobareu un camp anomenat "Tiempo funcionando" i un altre anomenat "Último arranque". Com ha obtingut Zenmap aquesta informació? Creieu que el valor que us dona és molt fiable?

9. **(0.5 punts)** Si utilitzeu "Topologia" → "Visor de anfitriones" per examinar les dades que heu obtingut sobre `wiki.uab.cat`, `venezia.uab.cat` i `www.uab.cat`, trobareu informació sobre el "TCP sequence index" i un

indicador de dificultat. Expliqueu qué vol dir i per a qué serveix aquest index de dificultat.

5 TOP Enginyeria

Tots els alumnes que obtinguin més del 75% de la puntuació possible als tres apartats identificats amb la icona de TOP Enginyeria [1], obtindran el mèrit mitjà "Nothing remains hidden", que reconeix el seu domini utilitzant escàners de xarxa.

6 Calendari i fites importants

A continuació es descriu el calendari de les fites relatives a la pràctica:

- **Sessió 1**: 27/03/17 i 30/03/17.
- **Sessió 2**: 3/04/17 i 6/04/17.
- **Entrega**: El dia abans a la següent pràctica (17/04/17 i 19/04/17).

7 Condicions de lliurament

- L'entrega de la pràctica es farà a través del campus virtual.
- Cada grup ha d'entregar un informe en format pdf que contingui les respostes a totes les preguntes d'aquest enunciat.
- No s'acceptarà cap informe lliurat fora de plaç.

Referències

[1] Departament d'Enginyeria de la Informació i les Comunicacions. TOP Enginyeria. `http://top.uab.cat`.

[2] nmap.org. NMAP - Free Security Scanner. `http://nmap.org/`.

[3] nmap.org. ZENMAP - Oficcial cross-platform NMAP GUI. http://nmap.org/zenmap/.

[4] SourceForge. Angry IP Scanner. http://angryip.org/w/Home.

[5] Wikipedia. NetBIOS. http://es.wikipedia.org/wiki/NetBIOS.