

ATTAQUE MAN-IN-THE-MIDDLE DE TYPE ARP SPOOFING



- 1. <u>Création des machines virtuelles :</u>
- 1.1 Créer chaque machine virtuelle (vous pouvez vous aider du document d'aide à la création d'une machine virtuelle sur le lien : http://newtonformationsnir.fr/TP/virtualbox.pdf)
- 2. <u>Relevé des adresses IP des machines virtuelles :</u>
- 2.1 Relever les adresses IP des machines virtuelles.
- IP1 :
- IP2 :
- IP3 :



3. Préparation de l'attaque :

Sur l'attaquant :

- 3.1 Réaliser un test de connexion (ping) depuis l'attaquant vers le serveur-web et le client Alice.
- 3.2 Relever le contenu de la table ARP sur l'attaquant.

Host	Adresse IP	Adresse MAC
Alice		
Serveur-web		

3.3 Relever le nom de l'interface réseau de l'attaquant.

Sur la cible Alice :

- 3.4 Réaliser un test de connexion (ping) depuis Alice vers le serveur-web et l'attaquant.
- 3.5 Relever le contenu de la table ARP sur la cible Alice.

Host	Adresse IP	Adresse MAC
Attaquant		
Serveur-web		

Sur le serveur web :

3.6 Réaliser un test de connexion (ping) depuis le serveur-web vers Alice et l'attaquant.

3.7 Relever le contenu de la table ARP sur le serveur web.

Host	Adresse IP	Adresse MAC
Attaquant		
Alice		

- 4. <u>Attaque ARP Spoofing :</u>
- 4.1 Effectuer l'attaque ARP Spoofing :

```
sudo ettercap -i nom_interface -T -M arp /IP serveur-web// /IP client//
```

Exemple : sudo ettercap –i enol –T –M arp /192.168.5.254// /192.168.5.128//

4.2 Relever de nouveau le contenu de la table ARP sur l'attaquant, la cible et le serveur web (pour l'attaquant, pensez à ouvrir un deuxième onglet du terminal).

Sur l'attaquant :

Host	Adresse IP	Adresse MAC
Alice		
Serveur-web		



Sur la cible Alice :

Host	Adresse IP	Adresse MAC
Attaquant		
Serveur-web		

Sur le serveur web :

Host	Adresse IP	Adresse MAC
Attaquant		
Alice		

- 4.3 Que constatez-vous ?
- 5. Analyse des données en transit:
- 5.1 Lancer Wireshark sur l'attaquant de façon à lire les données présentes sur son interface réseau (pour lancer wireshark sur debian : sudo wireshark).

Pour choisir l'interface réseau :

Activités	∠ Wireshark ▼ 24 févr. 18:13	∎♥∎▼
	L'analyseur de réseau Wireshark	×
<u>Fichier</u> Ed	liter <u>V</u> ue <u>A</u> ller <u>C</u> apture <u>A</u> nalyser <u>S</u> tatistiques Telephon <u>i</u> e <u>W</u> ireless <u>O</u> utils <u>A</u> ide	
	₫ 🐵 🚍 🖹 🕱 🗿 🗢 🗢 🛎 🖉 💆 📃 🔍 Q, Q, 🎞	
Apply a d	display filter <ctrl-></ctrl->	
	Welcome to Wireshark	
	Capture	
	using this filter: 📕 Enter a capture filter 🔹 All interfaces shown 👻	
	enp0s3	
	anyLAUM_ Loopback: lo	
	bluetooth-monitor	
	nfqueue	
	dbus-session	
	Cisco remote capture: ciscodump DisplayBort AUX chapped monitor capture: dpaysmon	
	Random packet generator: randpkt	
	systemd lournal Export: sdiournal	
	Learn	
	User's Guide · Wiki · Questions and Answers · Mailing Lists	
	You are running Wireshark 3.4.10 (Git v3.4.10 packaged as 3.4.10-0+deb11u1).	

5.2 Effectuer un filtre arp.

Pour appliquer un filtre :

Eichier Editer Vue Aller Capture Analyser Statistiques Telephonje Wireless Qutils Aide Image: All the statistic control of the statisticontec control of the statistic control of the	
Destination Protocol Length Info 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:09:027:21:15:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:09:027:21:15:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:09:09:07:21:15:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:09:09:07:21:15:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:09:01:07:15:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:09:01:07:15:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:09:10:02:15:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:09:10:02:15:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:09:10:02:15:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:09:10:02:15:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:08:100:12:13:5:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:08:100:12:13:5:5e 15e PcsComput.e8:06:192 ARP 42:10:9.2.7.15:at:08:100:12:13:5:5e	Saisir le filtre (ici arp) dans la zone indiquée et valider le filtrage en cliquant sur la flèche.



- 5.3 Observer et analyser les requêtes arp correspondant à l'attaque. Que constatezvous ?
- 5.4 Lancer le navigateur sur la machine Alice.
- 5.5 Modifier le filtrage pour appliquer un filtre http.
- 5.6 Effectuer une requête http depuis Alice vers le serveur-web. Pour cela, on saisit dans le navigateur : <u>http://IP1:3000</u> (avec IP1 : IP du serveur-web, 3000 est le port utilisé par ce serveur).
- 5.7 Sur wireshark, décoder la requête en sélectionnant, Analyser/Suivre/http stream

Activités 🖉 Wireshark 🔻	24 févr. 18:28	- •0 · ·
	*enp0s3	×
<u>F</u> ichier <u>E</u> diter <u>V</u> ue <u>A</u> ller <u>C</u> apture	Analyser Statistiques Telephonie Wireless	<u>O</u> utils <u>A</u> ide
	Display <u>F</u> ilters Afficher les Filtres <u>M</u> acros	€ € € ፻
📙 http	Display Filter Expression	+
No. Time Source 10 11.465151665 10.2.6 15 51.487536889 10.0.2.7 19 11.664361997 10.0.2.6 21 11.671276886 10.0.2.7	Appliquer en Colonne Ctrl+Maj+I Appliquer comme un Filtre Prepare as Filter Filtre de Conversation	th'Info 80 POST /login HTTP/1.1 , JavaScrij 91 HTTP/1.1 200 OK (text/html) 90 GET /dashboard HTTP/1.1 101 HTTP/1.1 304 Not Modified
	Protocoles activés Ctrl+Maj+E	
	Décoder <u>C</u> omme Ctrl+Maj+U	
	Recharger Plugins Lua Ctrl+Maj+L	
	SCTP >	
	Suivre >	
	Show Packet Bytes Ctrl+Maj+O	
4	Information Expert	
Frame 21: 330 bytes on wire (26. Ethernet II, Src: PcsCompu_11:4 Internet Protocol Version 4, Sr Transmission Control Protocol, s 10000 08 00 07 21 15 6 08 00 27 1010 01 30 64 24 40 00 40 66 bd 1020 02 06 06 bb 8 9e bB 80 bb be 1030 01 7 10 97 00 00 01 01 08 1040 27 91 48 54 65 02 71 12 02	40 bits), 330 bytes captured (2640 bits) or 7:3e (08:00:77:11:47:3e), Dst: PcsCompu_21: 5:10.02.77, Dst: 10.02.6 5rc Port: 3000, Dst Port: 40632, Seq: 254, 11 47 3e 08 00 45 00 · 1! ^ · · (G-E 82 0a 00 02 07 0a 00 · · · (G-0) 65 257 59 0F 180 18 · · · hRu 0a 07 24 10 c8 b0 8c · · S 31 20 33 30 42 04 e / HTTP/1. 304 N	interface enp0s3, id 0 15:5e (08:00:27:21:15:5e) Ack: 887, Len: 264

5.8 Relever le login/password.

Wireshark · Follow HTTP Stream (tcp.stream eq 1) · enp0s3	×
POST /login HTTP/1.1	
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	
Accept: */* Accept-Language: fr.fr-FR:g=0.8.en-US:g=0.5.en:g=0.3	
Accept-Encoding: gzip, deflate	
Referer: http://10.0.2.7:3000/	
Origin: http://10.0.2.7:3000	
Content-Length: 36	
connection: keep-alive	
{"login":"admin","password":"admin"}HTTP/1.1 200 OK	
X-Powered-By: Express Content_Type: text/html: charset=utf_R	
Content-Length: 25	
ETag: W/"19-1KqvnHy99aiGrXobx+cch2Vmm94"	
Date: Ind, 23 FeD 2023 If 21:22 UMI	_
Keep-Alive: timeout=5	
Authentification r. ussiGET /dashboard HTTP/1.1	
Host: 10.0.2.7:3000	
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0	
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3	
Accept-Encoding: gzip, deflate	
Connection: Keep-alive Referer: http://10.0.2.7:3000/	*