INFORME AUDITORÍA WIFI

DANIEL HIDALGO PAGÉS

INDICE

OBJETIVO

La auditoría Wi-Fi, también conocida como evaluación de la seguridad Wi-Fi, tiene como objetivo principal identificar las debilidades y vulnerabilidades de una red inalámbrica para que puedan ser corregidos, mejorando así su seguridad y su protección frente a posibles ataques. En el caso de la empresa ASOT, el objetivo de la auditoría Wi-Fi sería garantizar la protección de su red inalámbrica y la información confidencial de su empresa.

La evaluación de seguridad Wi-Fi de ASOT comenzaría con un análisis detallado de la configuración de la red inalámbrica y los dispositivos conectados a ella. El objetivo de esta fase es identificar los puntos débiles de la red, como contraseñas débiles, configuraciones incorrectas o dispositivos obsoletos.

A continuación, se realizaría un escaneo de la red inalámbrica para detectar la presencia de dispositivos no autorizados. El objetivo es identificar dispositivos que puedan representar una amenaza para la seguridad de la red, como enrutadores desconocidos o dispositivos móviles no autorizados.

Luego se realizaría un análisis de la calidad de la señal Wi-Fi para determinar si había áreas de la organización que no estaban cubiertas o eran vulnerables a posibles ataques de hackers cercanos. El objetivo es identificar estas áreas y tomar medidas para mejorar la cobertura y la seguridad.

La siguiente fase sería la prueba de penetración para simular ataques de piratería en la red inalámbrica de ASOT. El objetivo de estas pruebas es evaluar la capacidad de la red para soportar ataques externos y, si se encuentran vulnerabilidades, tomar medidas para corregirlas y mejorar la seguridad.

Finalmente, se elaboraría un informe detallado con las recomendaciones y medidas de seguridad a implementar para proteger la red inalámbrica ASOT. El objetivo de este informe es proporcionar a la empresa una guía clara sobre las medidas necesarias para garantizar la seguridad de su red Wi-Fi.

En resumen, el objetivo de la auditoría WiFi en ASOT es garantizar la protección de su red inalámbrica y la información corporativa confidencial mediante la identificación de vulnerabilidades y la implementación de las medidas de seguridad necesarias para mejorar la seguridad y proteger la red de posibles ataques de piratas informáticos.

ALCANCE Y LIMITACIONES

El alcance de una auditoría wifi en ASOT estaría determinado por los objetivos específicos que se establezcan para la evaluación de seguridad de la red inalámbrica. A continuación, se detallan los posibles objetivos y el alcance correspondiente:

- Identificación de vulnerabilidades: el alcance de la auditoría wifi sería la identificación de vulnerabilidades en la red inalámbrica de ASOT, tales como contraseñas débiles, configuraciones inadecuadas, dispositivos no autorizados y áreas con cobertura deficiente.
- Pruebas de penetración: el alcance de la auditoría wifi sería realizar pruebas de penetración para simular ataques de hackers a la red inalámbrica de ASOT, con el fin de evaluar la capacidad de la red para resistir ataques externos.
- Cumplimiento de normas y regulaciones: el alcance de la auditoría wifi sería evaluar si la red inalámbrica de ASOT cumple con las normas y regulaciones establecidas por organismos reguladores o leyes aplicables, como el RGPD (Reglamento General de Protección de Datos).

Las limitaciones de una auditoría wifi en ASOT estarían determinadas por diversos factores, como la complejidad de la red inalámbrica, la presencia de firewalls o políticas de seguridad restrictivas, el acceso limitado a algunos dispositivos o áreas de la empresa y la capacidad del equipo de auditoría para realizar pruebas avanzadas de seguridad. Además, algunas limitaciones específicas son:

- Limitaciones en el acceso: si algunos dispositivos o áreas de la empresa están restringidos o protegidos por firewalls, políticas de seguridad o controles de acceso físicos, la auditoría wifi podría verse limitada en cuanto al acceso y la capacidad de realizar pruebas exhaustivas.
- Limitaciones técnicas: si la red inalámbrica de ASOT es muy compleja o cuenta con dispositivos y tecnologías muy avanzados, la auditoría wifi podría verse limitada en cuanto a la capacidad del equipo de auditoría para realizar pruebas avanzadas de seguridad.
- Limitaciones de tiempo: si la auditoría wifi cuenta con un tiempo limitado para su realización, el alcance de la evaluación de seguridad podría verse limitado en función del tiempo disponible y de los objetivos prioritarios establecidos.
- Limitaciones en el presupuesto: si el presupuesto para la auditoría wifi es limitado, se podría ver limitado el alcance de la evaluación y la capacidad del equipo de auditoría para realizar pruebas avanzadas de seguridad o para implementar medidas de seguridad adicionales.

En resumen, el alcance de una auditoría wifi en ASOT dependería de los objetivos específicos establecidos para la evaluación de seguridad de la red inalámbrica, mientras que las limitaciones estarían determinadas por diversos factores como el acceso, la complejidad de la red, el tiempo disponible, el presupuesto y la capacidad del equipo de auditoría.

METODOLOGÍA

Existen varias metodologías para realizar una auditoría wifi, pero a continuación se describirá una posible metodología que se podría utilizar en una auditoría wifi en ASOT:

1. Planificación: en esta fase se definirían los objetivos de la auditoría wifi, se determinaría el alcance y las limitaciones, se seleccionaría el equipo de auditoría y se establecerían las fechas y horarios para la evaluación.
2. Recopilación de información: en esta fase se recopilaría información relevante sobre la red inalámbrica de ASOT, como la topología de la red, el número de dispositivos conectados, los protocolos de seguridad utilizados, los puntos de acceso (AP) disponibles, entre otros.
3. Identificación de dispositivos: en esta fase se identificarían los dispositivos que se encuentran conectados a la red inalámbrica de ASOT y se evaluaría si los mismos están autorizados o no para estar en la red.
4. Análisis de vulnerabilidades: en esta fase se analizarían las vulnerabilidades de la red inalámbrica, se evaluarían los protocolos de seguridad utilizados, se revisarían las configuraciones de los dispositivos de red y se realizarían pruebas de penetración para identificar posibles vulnerabilidades.
5. Evaluación de seguridad: en esta fase se evaluaría la seguridad de la red inalámbrica de ASOT y se identificarían posibles amenazas o riesgos para la red, así como también se evaluaría la efectividad de las medidas de seguridad implementadas.
6. Documentación: en esta fase se documentaría el proceso de auditoría wifi, se elaborarían informes detallados sobre las vulnerabilidades y riesgos encontrados, se realizaría un informe de recomendaciones y se presentarían los hallazgos a la empresa ASOT.
7. Implementación de medidas de seguridad: en esta fase se implementarían medidas de seguridad adicionales para mejorar la seguridad de la red inalámbrica de ASOT, basándose en las recomendaciones realizadas en el informe de auditoría wifi.

PRUEBAS REALIZADAS

En una auditoría wifi, se pueden realizar diversas pruebas para evaluar la seguridad de la red inalámbrica de la empresa ASOT.

En este caso se han analizado todas las redes inalámbricas centrándonos en las redes con los nombres de “ASOT-WiFi-XXX”.

Al hacer esto ya encontramos varias vulnerabilidades que pueden ser críticas para la empresa:

```
48:4A:E9:EC:21:63  -64        2        0    0   6  130   OPN              wOffice
CC:ED:DC:F8:B8:E8  -59        4        0    0   6  130   WPA2 CCMP   PSK  MOVISTAR_B8E8
48:4A:E9:EB:93:24  -60        3        0    0  11  130   WPA2 CCMP   PSK  wSystems
F8:5B:3B:FE:83:1F  -63        0        2    0  11  130   WPA2 CCMP   PSK  MOVISTAR_8310
48:4A:E9:EB:93:22  -72        2        0    0  11  130   OPN              wGuest_Cesur
48:4A:E9:EB:72:E2  -81        2        0    0  11  130   OPN              wGuest_Cesur
F8:8E:85:CC:EE:3E  -36       10        0    0   7   54e  WPA2 TKIP   PSK  ASOT-WiFi-001
30:DE:4B:83:8F:F8  -30        3        0    0   3  270   WPA2 CCMP   PSK  ASOT-WiFi-006
48:4A:E9:EB:93:21  -59        4        0    0  11  130   OPN              wTeacher
48:4A:E9:EC:59:64  -44        3        0    0  11  130   WPA2 CCMP   PSK  wSystems
48:4A:E9:EC:59:61  -46        3        0    0  11  130   OPN              wTeacher
48:4A:E9:EB:72:E1  -64        3        0    0  11  130   OPN              wTeacher
48:4A:E9:EC:59:63  -43        3        0    0  11  130   OPN              wOffice
48:4A:E9:EB:72:E4  -64        3        0    0  11  130   WPA2 CCMP   PSK  wSystems
48:4A:E9:EB:72:E3  -64        4        0    0  11  130   OPN              wOffice
30:DE:4B:83:8E:C6  -23        1        0    0   2  270   WPA2 CCMP   PSK  TP-Link_8EC6
F8:8E:85:C7:FA:7B  -15       15        1    0   4  130   WPA2 CCMP   PSK  ASOT-WiFi-003
48:4A:E9:EB:54:61  -63        3        0    0   6  130   OPN              wTeacher
E2:BF:CE:07:99:09  -35        8        0    0   3  180   WPA2 CCMP   PSK  ASOT-WiFi-011
F8:8E:85:C7:C5:92  -24        8        0    0   3   54e  WPA2 TKIP   PSK  ASOT-WiFi-002
C4:A3:66:D0:5B:EC  -32        8        0    0   3   11e. WPA2 CCMP   PSK  ASOT-WiFi-009
48:4A:E9:EE:30:C2  -79        2        0    0   1  130   OPN              wGuest_Cesur
0C:8E:29:AE:3A:9A  -30        6        0    0   1  130   WPA2 CCMP   PSK  ASOT-WiFi-010
B4:F7:A1:D0:F4:60  -48        7        0    0   3   65   WPA2 CCMP   PSK  ASOT-WiFi-011
F8:8E:85:CC:D0:20  -27       17        0    0   3   54e  WPA2 TKIP   PSK  ASOT-Wifi-004
30:DE:4B:83:8F:C8  -33       12        0    0   9  270   WPA2 CCMP   PSK  Wifi_EH_007
30:DE:4B:83:8E:D8  -40        6        0    0   3  270   WPA2 CCMP   PSK  Wifi-HE-005
```

Se detectaron un total de 11 redes wifi protegidas mediante WPA2.

Se puede observar como el nombre de la red SSID, BSSID, canal...

Nos piden que analicemos en profundidad la red wifi con el nombre “ASOT-WIFI-001”, y observamos lo siguiente:

```
┌──(root㉿kali)-[/home/daniel]
└─# airodump-ng wlan0
```

```
CH  7 ][ Elapsed: 1 min ][ 2023-03-16 18:56

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

F8:8E:85:CC:EE:3E  -23  10       69        7    0   7   54e  WPA2 TKIP   PSK  ASOT-WiFi-001

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

F8:8E:85:CC:EE:3E  AE:41:42:5E:12:0B  -53    0 -54e     0        3         ASOT-WiFi-001
F8:8E:85:CC:EE:3E  7E:5B:0B:7C:ED:04  -35   54e- 1      0       22
(not associated)   AA:49:88:83:5C:31  -82    0 - 6      0        2
(not associated)   46:71:2F:57:DE:D5  -73    0 - 1      0        1
(not associated)   02:00:00:00:00:00  -71    0 - 1      3        2
(not associated)   CE:72:C4:41:A6:E8  -37    0 - 1      0        6
(not associated)   8E:AD:0D:45:8D:B6  -43    0 - 1      0        1
(not associated)   62:46:44:8F:B8:78  -45    0 - 1      0        1
(not associated)   E8:2A:EA:22:0F:A1  -35    0 - 1      0       10         Wclassrooms
(not associated)   4A:03:A1:FD:4D:7D  -65    0 - 1      0        1
(not associated)   86:8B:28:98:96:8E  -69    0 - 1      0        1
(not associated)   5C:3A:45:F6:4E:4F  -41    0 - 1      0       15
(not associated)   EE:1D:7A:CD:2F:9C  -69    0 - 1      0        1
(not associated)   A0:AF:BD:13:65:8C  -13    0 - 1      0        9
(not associated)   9E:62:E1:06:E7:AE  -67    0 - 1      0        1
(not associated)   CA:18:4F:6B:1D:87  -63    0 - 1      0        1
(not associated)   06:F2:1F:29:B4:3D  -63    0 - 1      0        1
(not associated)   32:59:3C:13:C6:C5  -63    0 - 1      0        1
(not associated)   0C:C6:FD:12:CD:1D  -59    0 - 1      0        1
(not associated)   0E:C8:FB:15:20:53  -69    0 - 1      0        1
(not associated)   96:F1:EE:E7:B0:6F  -67    0 - 1      0        1
(not associated)   4E:87:DC:08:28:52  -76    0 - 6      0        1         Viva_cable25813
```

EXPLICACIÓN DE VULNERABILIDADES

Tras analizar las distintas redes de la empresa podemos observar:

- Las redes tienen un nombre muy similar que incluye el propio nombre de la empresa dando información de la misma y un SSID muy parecido.
- Se utiliza el mismo patrón para las contraseñas, cambiando los últimos caracteres de esta forma “System!XXX” donde las “X” son los últimos caracteres, esto facilita mucho a los hackers hacer ataques por diccionario.
- Para terminar las contraseñas son bastante sencillas lo que puede suponer problemas.

CONTRASEÑA CRACKEADA

Dado a la falta de tiempo, y posiblemente de conocimiento para hacerlo de forma eficaz, no he sido capaz de crackear la contraseña, pero la herramienta a utilizar sería hashcat creando nuestro propio diccionario con reglas y obteniéndola sacando “System!y22”.