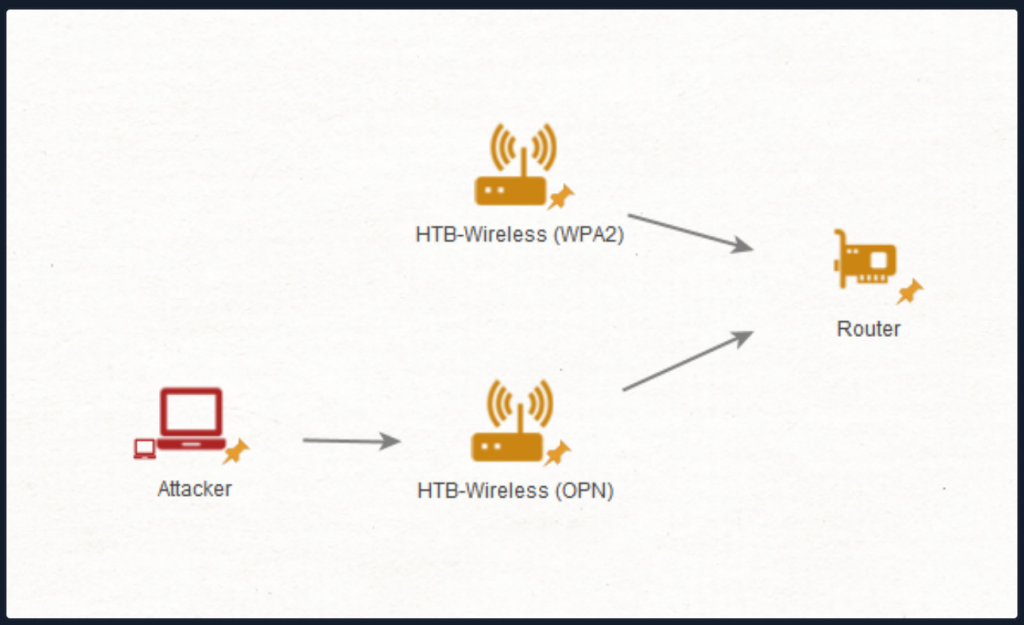
Rogue Access Point & Evil-Twin Attacks

Related PCAP File(s):

- `rogueap.cap`

Addressing rogue access points and evil-twin attacks can seem like a gargantuan task due to their often elusive nature. Nevertheless, with the appropriate strategies in place, these illegitimate access points can be detected and managed effectively. In the realm of malevolent access points, rogue and evil-twin attacks invariably surface as significant concerns.



A rogue access point primarily serves as a tool to circumvent perimeter controls in place. An adversary might install such an access point to sidestep network controls and segmentation barriers, which could, in many cases, take the form of hotspots or tethered connections. These rogue points have even been known to infiltrate air-gapped networks. Their primary function is to provide unauthorized access to restricted sections of a network. The critical point to remember here is that rogue access points are directly connected to the network.

Evil-Twin

An evil-twin on the other hand is spun up by an attacker for many other different purposes. The key here, is that in most cases these access points are not connected to our network. Instead, they are standalone access points, which might have a web server or something else to act as a man-in-the-middle for wireless clients.

Attackers might set these up to harvest wireless or domain passwords among other pieces of information. Commonly, these attacks might also encompass a hostile portal attack.

Airodump-ng Detection

Right away, we could utilize the ESSID filter for Airodump-ng to detect Evil-Twin style access points.

Rogue Access Point & Evil-Twin Attacks

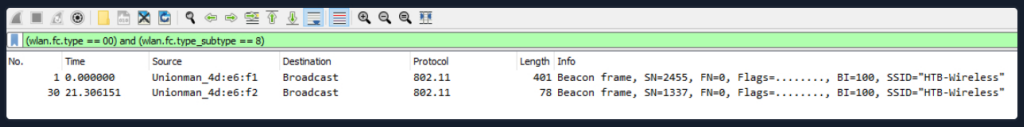
```
MisaelMacias@htb[/htb]$ sudo airodump-ng -c 4 --essid HTB-Wireless wlan0 -w raw

 CH  4 ][ Elapsed: 1 min ][ 2023-07-13 16:06
 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID
 F8:14:FE:4D:E6:F2   -7 100      470      155    0   4   54   OPN              HTB-Wireless
 F8:14:FE:4D:E6:F1   -5  96      682        0    0   4  324   WPA2 CCMP   PSK  HTB-Wireless
```

The above example would show that in fact an attacker might have spun up an open access point that has an identical ESSID as our access point. An attacker might do this to host what is commonly referred to as a hostile portal attack. A hostile portal attack is used by attackers in order extract credentials from users among other nefarious actions.

We might also want to be vigilant about deauthentication attempts, which could suggest enforcement measures from the attacker operating the evil-twin access point.

To conclusively ascertain whether this is an anomaly or an Airodump-ng error, we can commence our traffic analysis efforts (`rogueap.cap`). To filter for beacon frames, we could use the following.

- `(wlan.fc.type == 00) and (wlan.fc.type_subtype == 8)`



Beacon analysis is crucial in differentiating between genuine and fraudulent access points. One of the initial places to start is the `Robust Security Network (RSN)` information. This data communicates valuable information to clients about the supported ciphers, among other things.

Suppose we wish to examine our legitimate access point's RSN information.

```
IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (365 bytes)
    > Tag: SSID parameter set: "HTB-Wireless"
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 4
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: Country Information: Country Code US, Environment All
    > Tag: Power Constraint: 0
    > Tag: TPC Report Transmit Power: 22, Link Margin: 0
    > Tag: Tx Power Envelope
    > Tag: RM Enabled Capabilities (5 octets)
    > Tag: AP Channel Report: Operating Class 81, Channel List : 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11,
    > Tag: ERP Information
    > Tag: Extended Supported Rates 6, 12, 24, 48, [Mbit/sec]
    v Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 24
        RSN Version: 1
```

OFFLINE

Start Instance

∞ / 1 spawns left

```
> Group Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
  Pairwise Cipher Suite Count: 2
> Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) TKIP 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 1
> Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
> RSN Capabilities: 0x0000
```

It would indicate that WPA2 is supported with AES and TKIP with PSK as its authentication mechanism. However, when we switch to the illegitimate access point's RSN information, we may find it conspicuously missing.

```
> Frame 30: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> IEEE 802.11 Beacon frame, Flags: ........
v IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  v Tagged parameters (42 bytes)
    > Tag: SSID parameter set: "HTB-Wireless"
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 4
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    > Tag: ERP Information
    > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
```

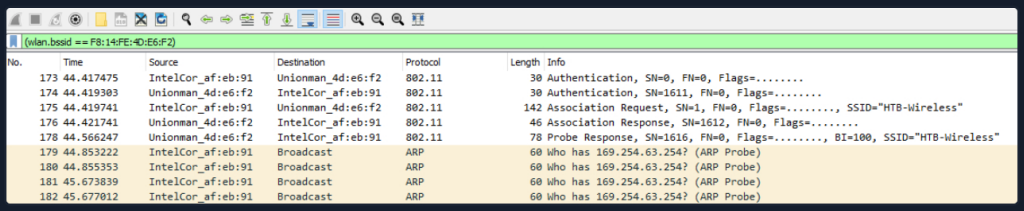
In most instances, a standard evil-twin attack will exhibit this characteristic. Nevertheless, we should always probe additional fields for discrepancies, particularly when dealing with more sophisticated evil-twin attacks. For example, an attacker might employ the same cipher that our access point uses, making the detection of this attack more challenging.

Under such circumstances, we could explore other aspects of the beacon frame, such as vendor-specific information, which is likely absent from the attacker's access point.

Finding a Fallen User

Despite comprehensive security awareness training, some users may fall prey to attacks like these. Fortunately, in the case of open network style evil-twin attacks, we can view most higher-level traffic in an unencrypted format. To filter exclusively for the evil-twin access point, we would employ the following filter.

- `(wlan.bssid == F8:14:FE:4D:E6:F2)`



If we detect ARP requests emanating from a client device connected to the suspicious network, we would identify this as a potential compromise indicator. In such instances, we should record pertinent details about the client device to further our incident response efforts.

1. `Its MAC address`
2. `Its host name`

Consequently, we might be able to instigate password resets and other reactive measures to prevent further infringement of our environment.

Finding Rogue Access Points

On the other hand, detecting rogue access points can often be a simple task of checking our network device lists. In the case of hotspot-based rogue access points (such as Windows hotspots), we might scrutinize wireless networks in our immediate vicinity. If we encounter an unrecognizable wireless network with a strong signal, particularly if it lacks encryption, this could indicate that a user has established a rogue access point to navigate around our perimeter controls.

Connect to Pwnbox
Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 138ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

+ 1 Inspect the rogueap.cap file, part of this module's resources, and enter the MAC address of the Evil Twin attack's victim as your answer.

2c:6d:c1:af:eb:91

Submit

← Previous Next →

Mark Complete & Next