Ex130 Submission

Gary Jones

Contents

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 cannect 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 hypertext link /Corp/message.txt (see figures 12 and 13).

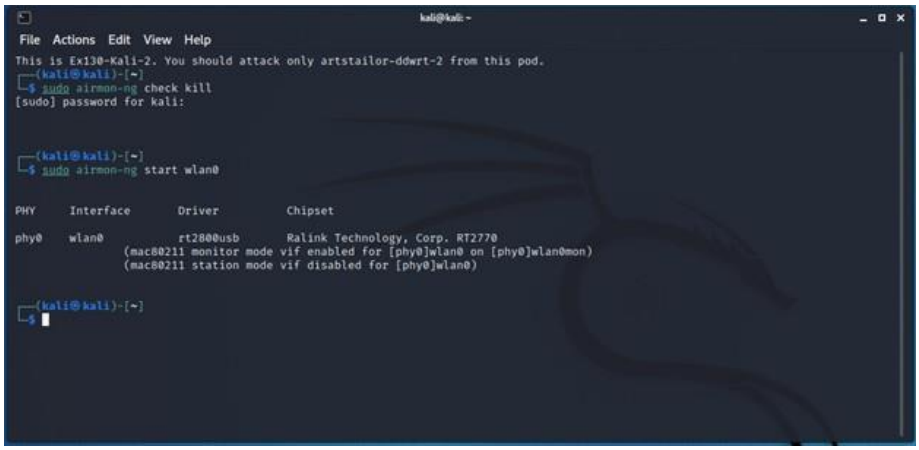


Figure 1:

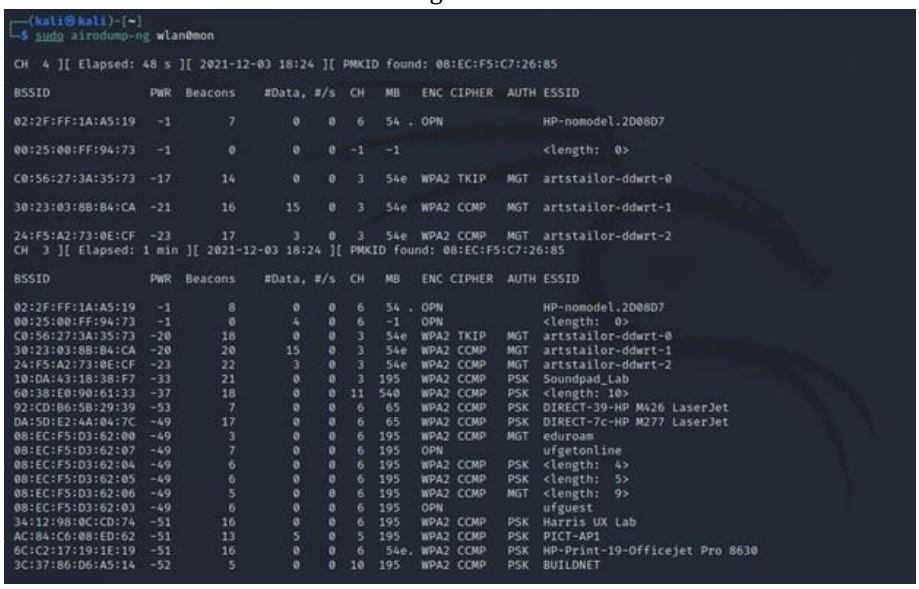


Figure 2:

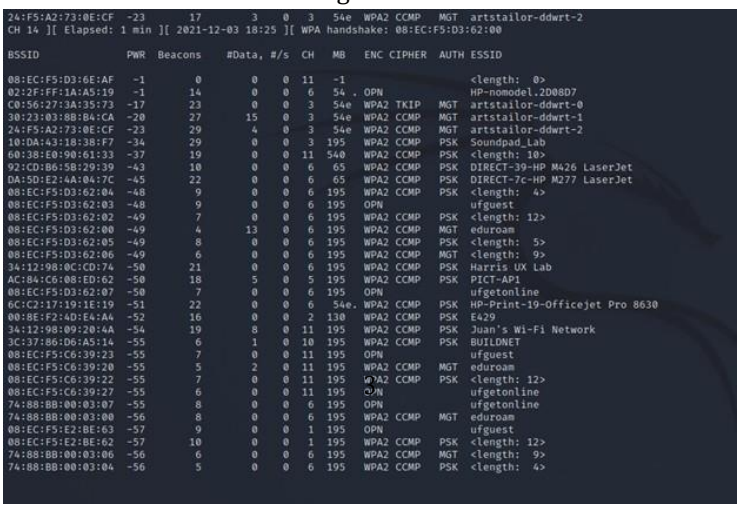


Figure 3:

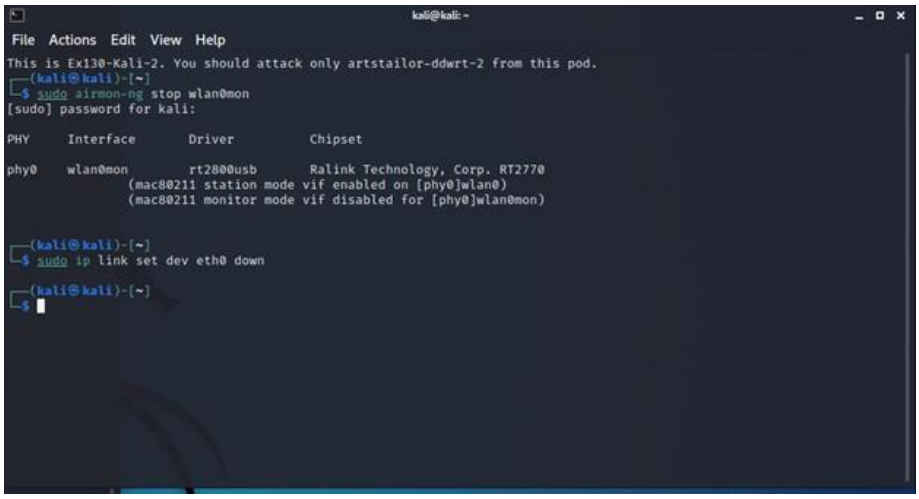


Figure 4:

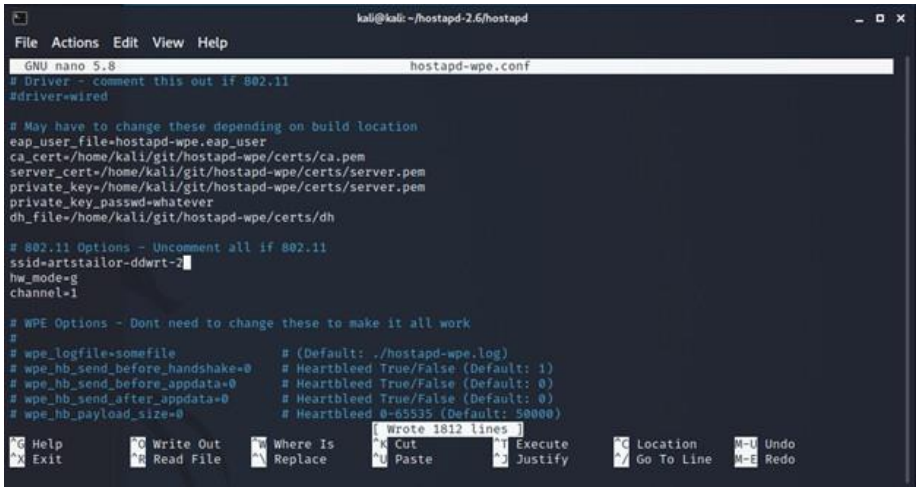


Figure 5:

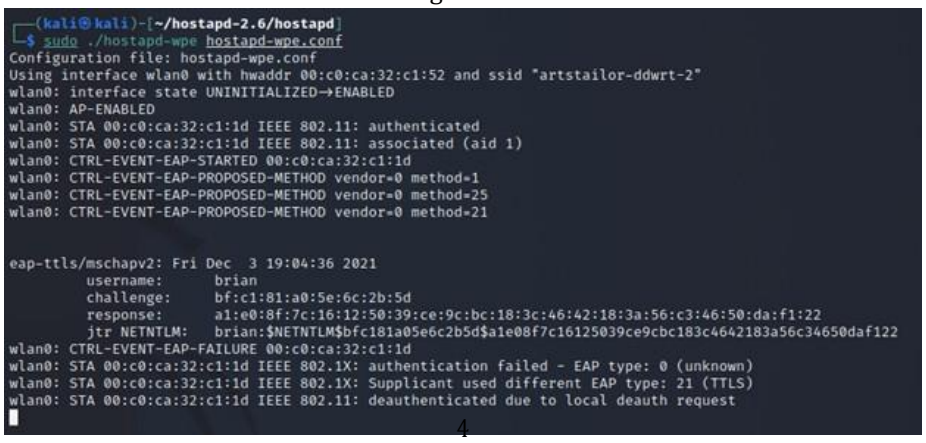


Figure 6:

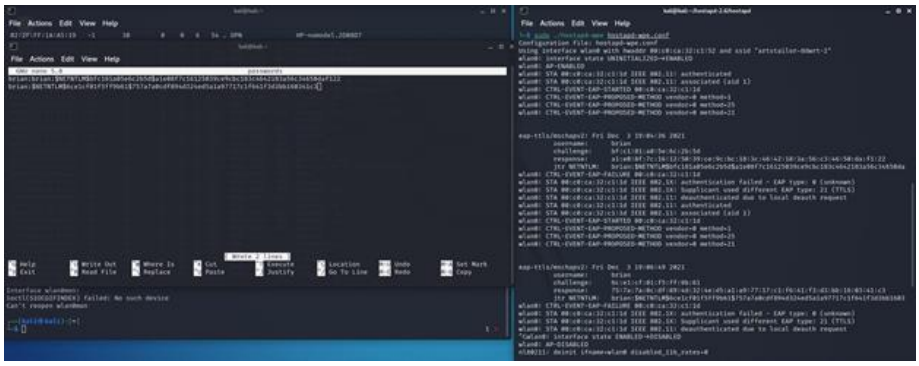


Figure 7:

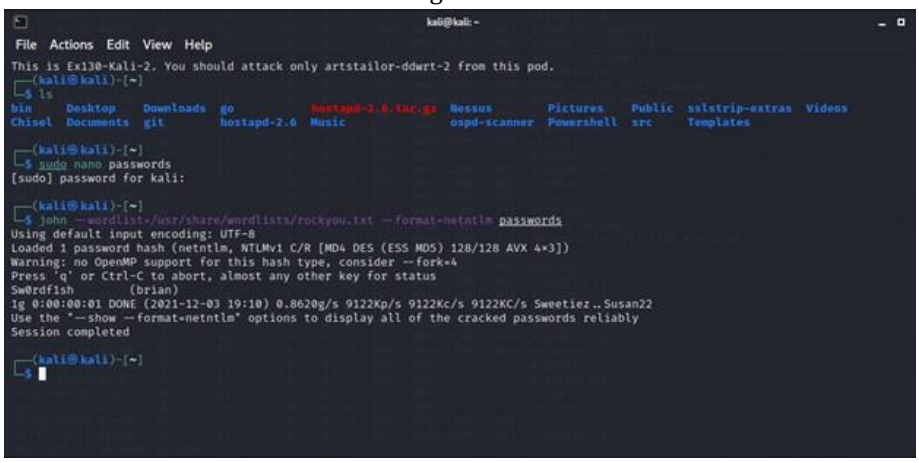


Figure 8:

Figure 9:

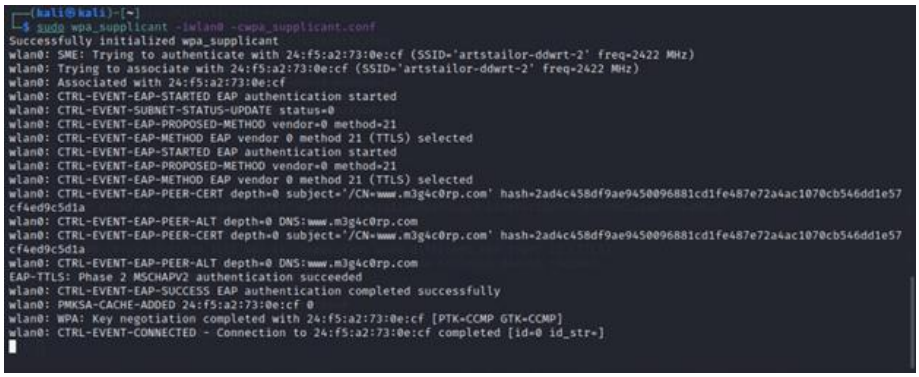


Figure 10:

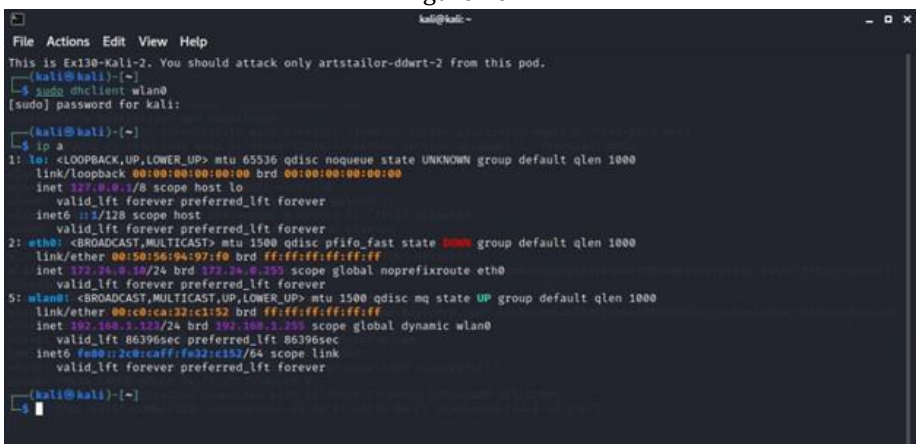
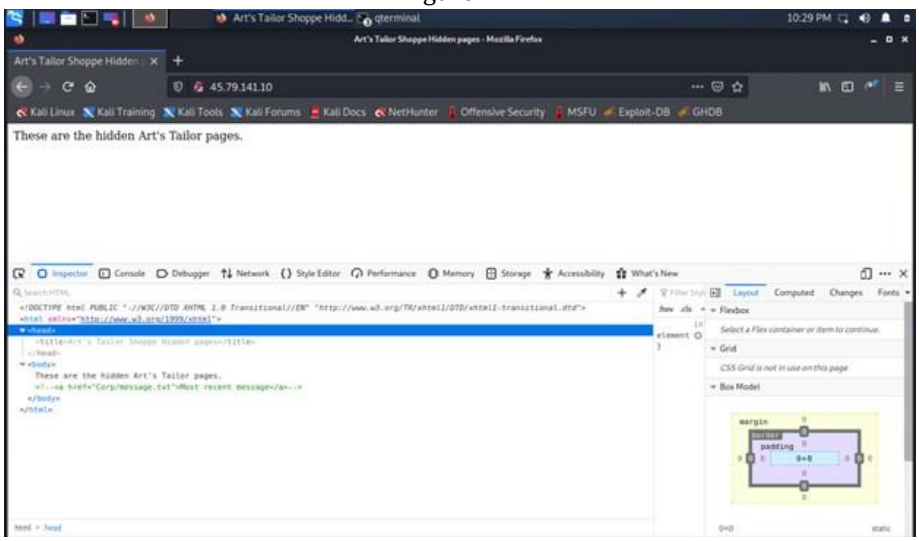


Figure 11:



Figur$_{6}$e 12:

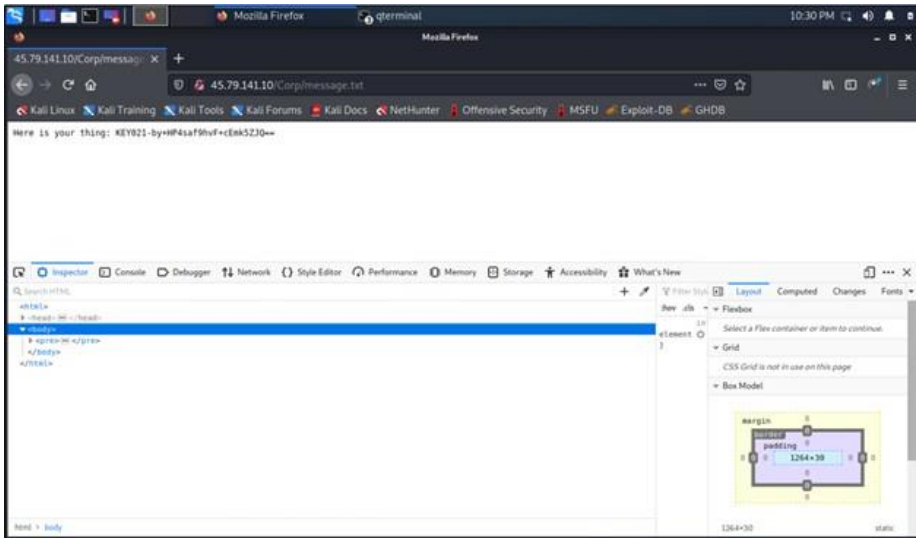

Mozilla Firefox
qterminal
10:30 PM
45.79.141.10/Corp/message.txt
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
GHDB
Here is your thing: KEY021-by+HP4saf9hvF+cEmk5ZJO==
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
What's New
Layout
Computed
Changes
Fonts
Flexbox
Grid
Box Model
margin
border
padding
1264×30

Figure 13: