

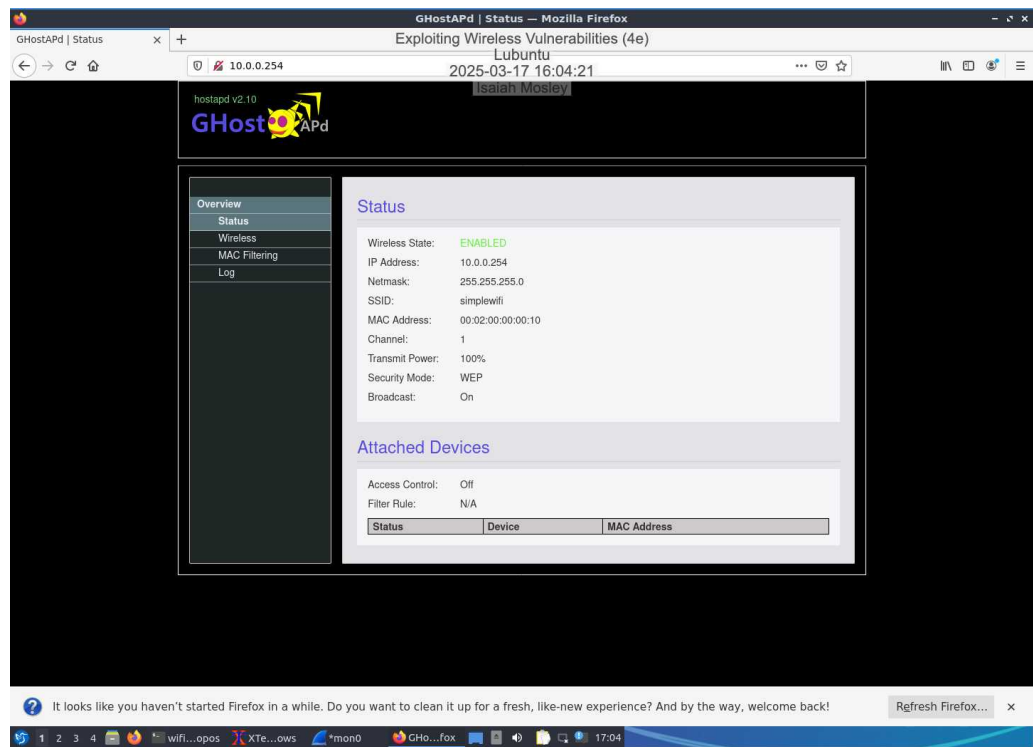
## Ethical Hacking, Fourth Edition - Lab 07

isaiahmosley80@gmail.com

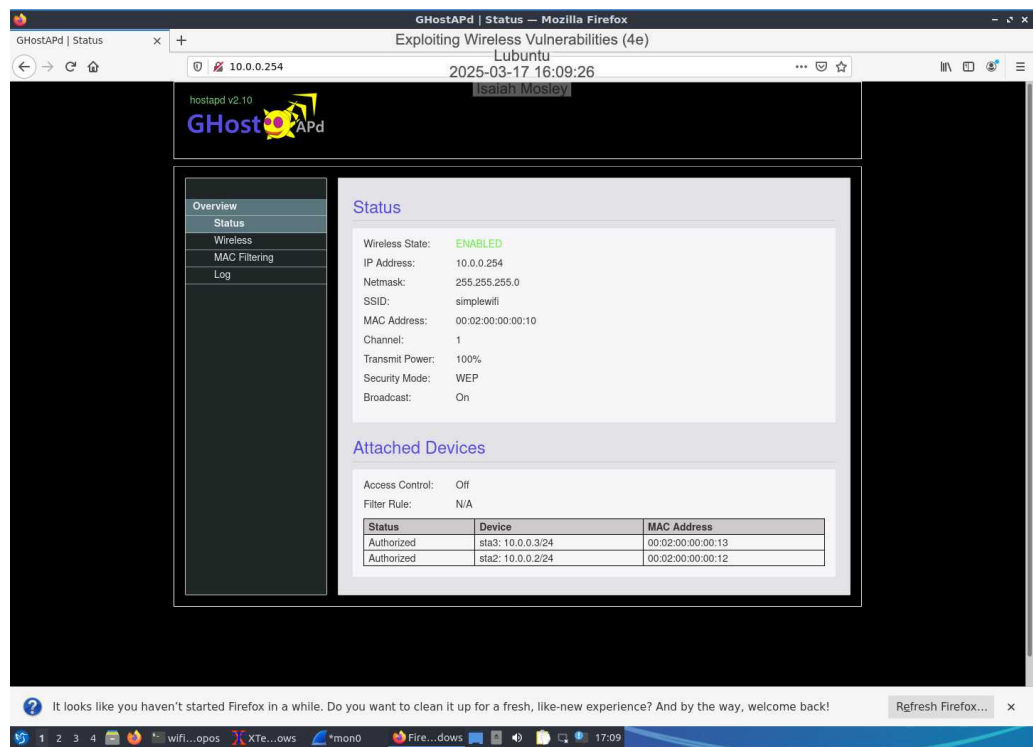
64%

Page 1 of 8

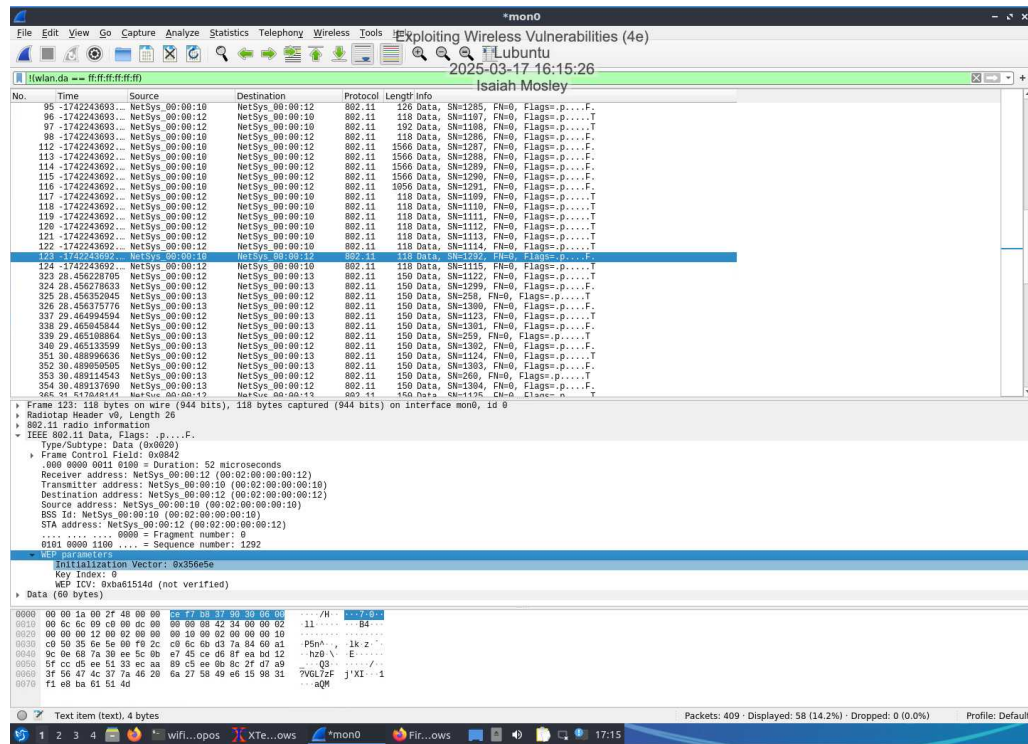
7. Make a screen capture showing WEP mode enabled on the GHostAPd Status page.



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.

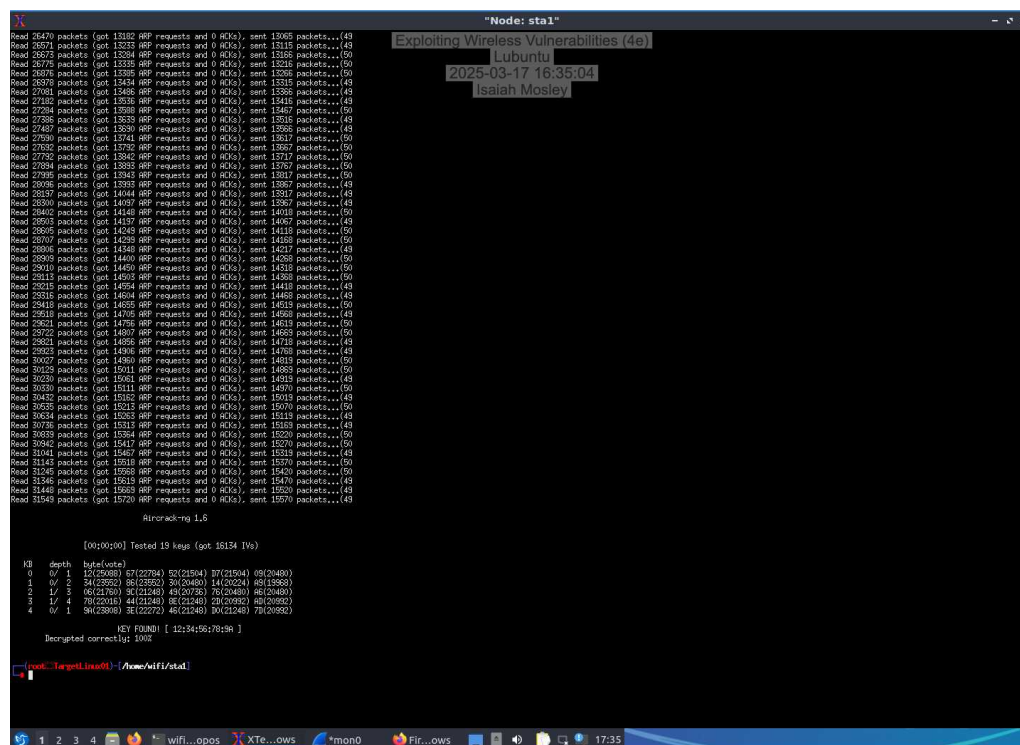


## Part 3: Break WEP Encryption

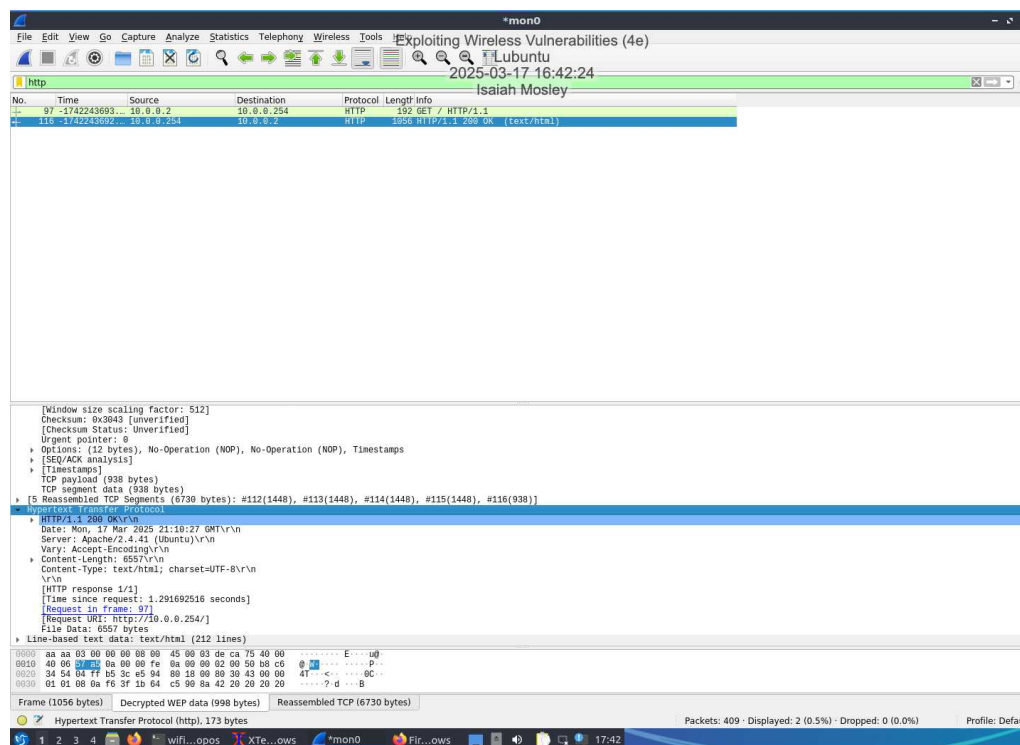
## Ethical Hacking, Fourth Edition - Lab 07

Ethical Hacking, Fourth Edition - Lab 07

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



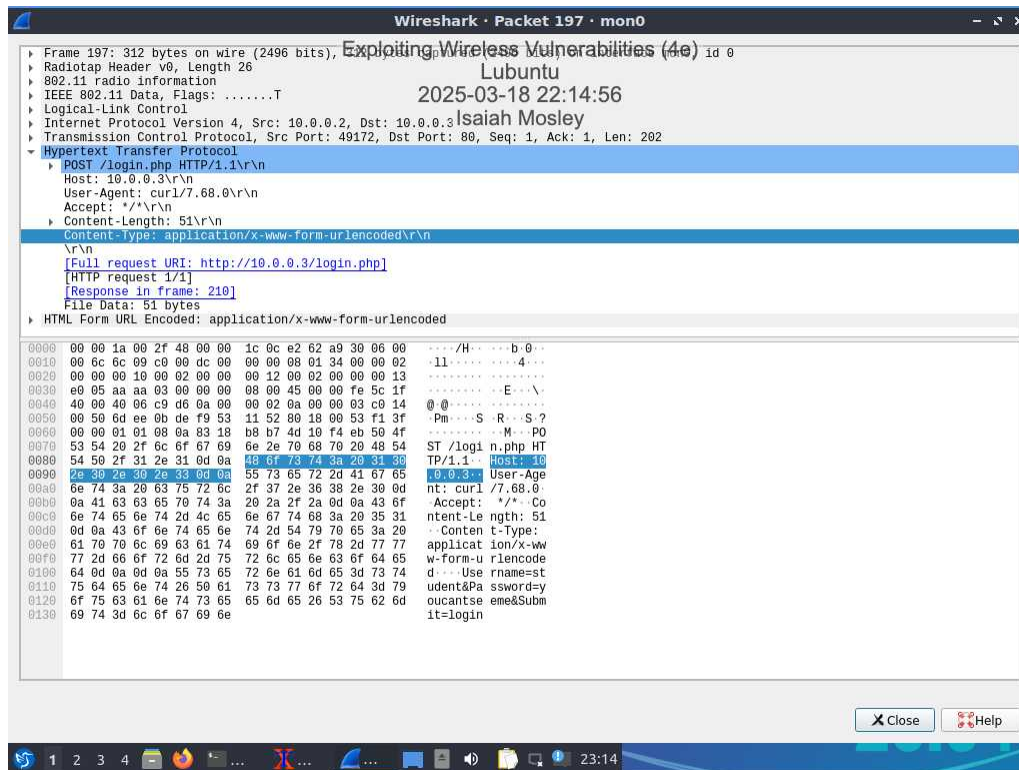
27. **Make a screen capture** showing the **decrypted Hypertext Transfer Protocol** data.



## Section 2: Applied Learning

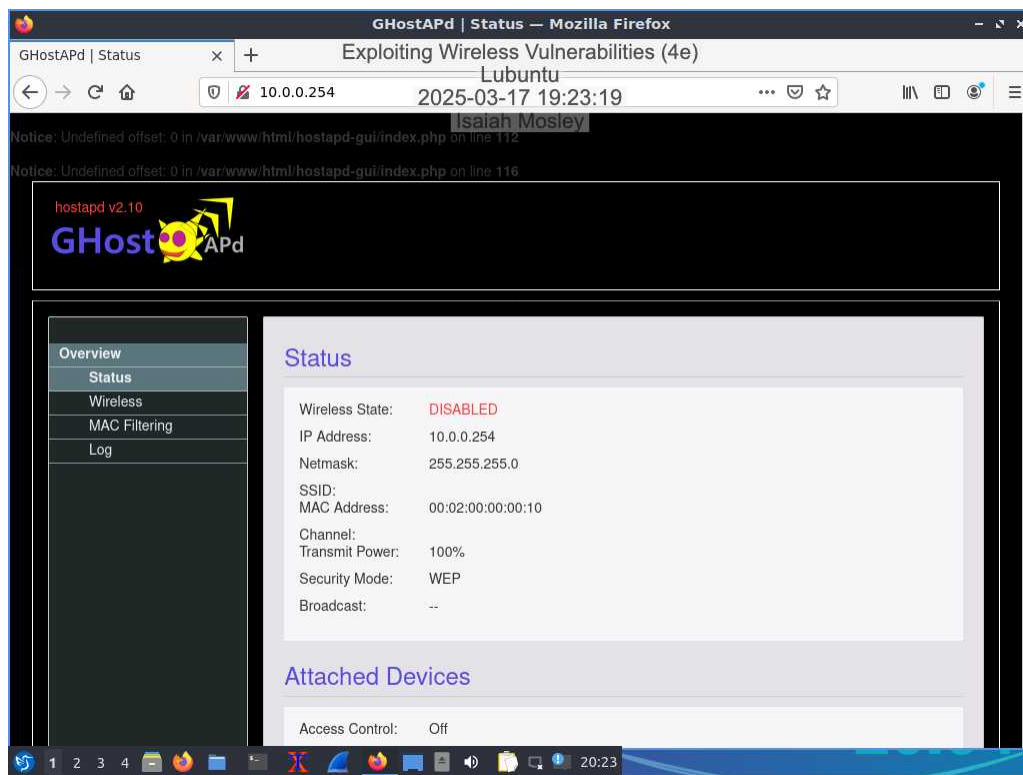
### Part 1: Capture Unencrypted Traffic with Wireshark

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**.

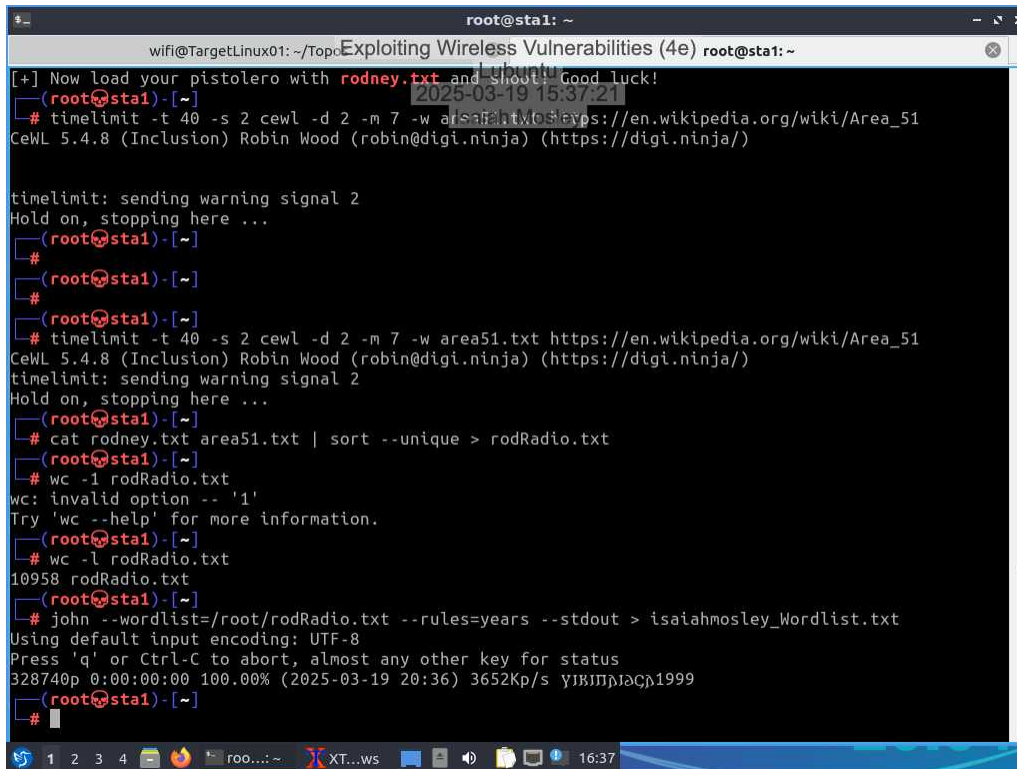


21. Make a screen capture showing the **CCMP Ext. Initialization Vector** in the **Packet Details** pane.

Incomplete

## 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: ~  
[+] Now load your pistolero with rodney.txt and shoot! Good Luck!  
(root@sta1)-[~]  
# timelimit -t 40 -s 2 cewl -d 2 -m 7 -w isaiahmosley://en.wikipedia.org/wiki/Area_51  
CeWL 5.4.8 (Inclusion) Robin Wood (robin@dig.ninja) (https://dig.ninja/)  
  
timelimit: sending warning signal 2  
Hold on, stopping here ...  
(root@sta1)-[~]  
#  
(root@sta1)-[~]  
#  
(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@dig.ninja) (https://dig.ninja/)  
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 -- 'l'  
Try 'wc --help' for more information.  
(root@sta1)-[~]  
# wc -l rodRadio.txt  
10958 rodRadio.txt  
(root@sta1)-[~]  
# john --wordlist=/root/rodRadio.txt --rules=years --stdout > isaiahmosley_Wordlist.txt  
Using default input encoding: UTF-8  
Press 'q' or Ctrl-C to abort, almost any other key for status  
328740p 0:00:00:00 100.00% (2025-03-19 20:36) 3652Kp/s уїтпїяєєр1999  
(root@sta1)-[~]  
#
```

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

Incomplete

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

Incomplete



### 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**.

Incomplete

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

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

Incomplete