

Exploiting Wireless Vulnerabilities (4e)

Ethical Hacking, Fourth Edition - Lab 07

Student:

Isaiah Mosley

Email:

isaiahmosley80@gmail.com

Time on Task:

78 hours, 31 minutes

Progress:

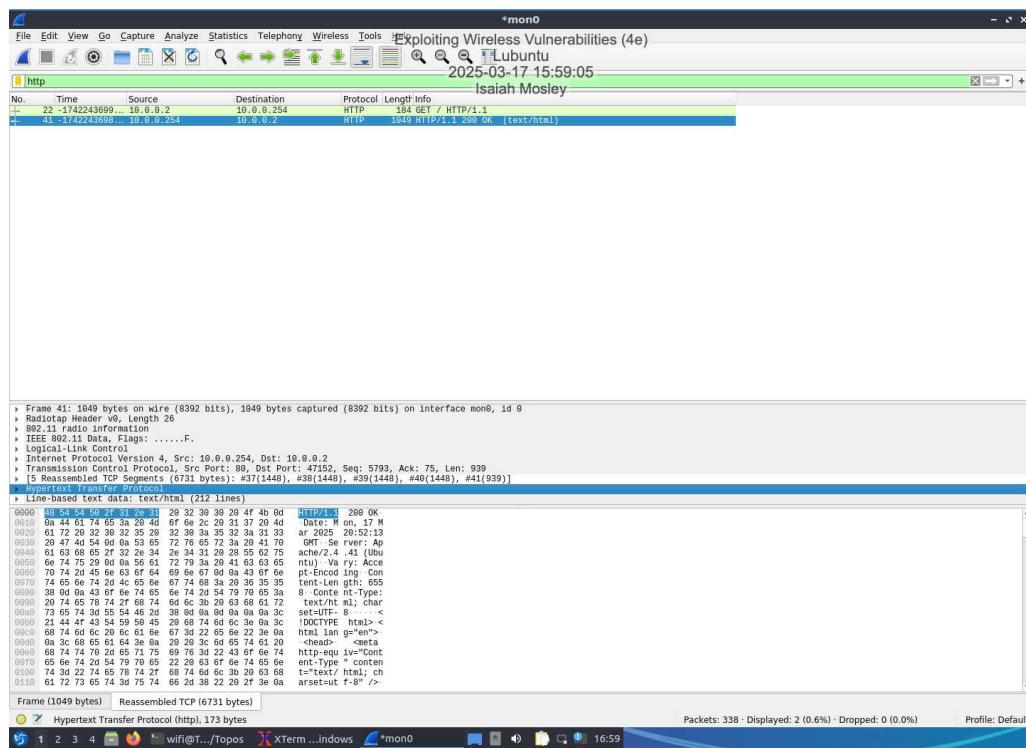
64%

Report Generated: Tuesday, December 2, 2025 at 1:24 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

Exploiting Wireless Vulnerabilities (4e)

Ethical Hacking, Fourth Edition - Lab 07

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

The screenshot shows the GHostAPd Status page in Mozilla Firefox. The title bar reads "GHostAPd | Status – Mozilla Firefox" and the address bar shows "10.0.0.254". The main content area has a sidebar on the left with "Overview" selected, showing "Status", "Wireless", "MAC Filtering", and "Log". The main panel displays the "Status" section with the following information:

Wireless State:	ENABLED
IP Address:	10.0.0.254
Netmask:	255.255.255.0
SSID:	simplewifi
MAC Address:	00:02:00:00:00:10
Channel:	1
Transmit Power:	100%
Security Mode:	WEP
Broadcast:	On

Below the status section is the "Attached Devices" section, which currently shows no devices attached.

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

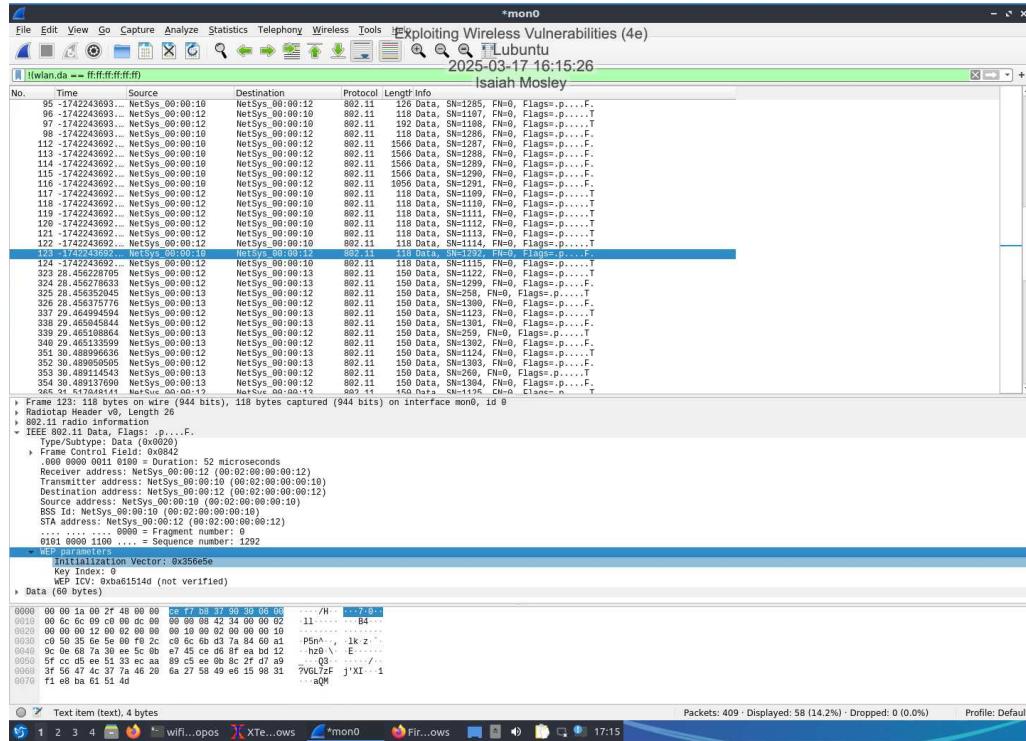
The screenshot shows the GHostAPd Status page in Mozilla Firefox, identical to the previous one but with two devices attached. The "Attached Devices" section now lists two entries:

Status	Device	MAC Address
Authorized	sta3: 10.0.0.3/24	00:02:00:00:00:13
Authorized	sta2: 10.0.0.2/24	00:02:00:00:00:12

Exploiting Wireless Vulnerabilities (4e)

Ethical Hacking, Fourth Edition - Lab 07

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



Part 3: Break WEP Encryption

Exploiting Wireless Vulnerabilities (4e)

Ethical Hacking, Fourth Edition - Lab 07

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

```
"Node: sta1"
Exploiting Wireless Vulnerabilities (4e)          Lubuntu 2025-03-17 16:35:04
Isaiah Mosley

Read 26470 packets (got 13182 RFP requests and 0 RCKs), sent 13065 packets... (49)
Read 26571 packets (got 13233 RFP requests and 0 RCKs), sent 13115 packets... (49)
Read 26672 packets (got 13284 RFP requests and 0 RCKs), sent 13126 packets... (50)
Read 26773 packets (got 13335 RFP requests and 0 RCKs), sent 13216 packets... (50)
Read 26874 packets (got 13386 RFP requests and 0 RCKs), sent 13296 packets... (50)
Read 26975 packets (got 13437 RFP requests and 0 RCKs), sent 13376 packets... (49)
Read 27076 packets (got 13488 RFP requests and 0 RCKs), sent 13456 packets... (49)
Read 27177 packets (got 13539 RFP requests and 0 RCKs), sent 13516 packets... (49)
Read 27278 packets (got 13590 RFP requests and 0 RCKs), sent 13596 packets... (49)
Read 27379 packets (got 13631 RFP requests and 0 RCKs), sent 13616 packets... (49)
Read 27480 packets (got 13672 RFP requests and 0 RCKs), sent 13696 packets... (49)
Read 27581 packets (got 13713 RFP requests and 0 RCKs), sent 13717 packets... (50)
Read 27682 packets (got 13754 RFP requests and 0 RCKs), sent 13719 packets... (50)
Read 27783 packets (got 13795 RFP requests and 0 RCKs), sent 13717 packets... (50)
Read 27884 packets (got 13836 RFP requests and 0 RCKs), sent 13719 packets... (50)
Read 27985 packets (got 13876 RFP requests and 0 RCKs), sent 13817 packets... (50)
Read 28086 packets (got 13917 RFP requests and 0 RCKs), sent 13897 packets... (49)
Read 28187 packets (got 13958 RFP requests and 0 RCKs), sent 13937 packets... (49)
Read 28288 packets (got 14009 RFP requests and 0 RCKs), sent 13957 packets... (49)
Read 28389 packets (got 14050 RFP requests and 0 RCKs), sent 14037 packets... (49)
Read 28490 packets (got 14091 RFP requests and 0 RCKs), sent 14067 packets... (49)
Read 28591 packets (got 14142 RFP requests and 0 RCKs), sent 14118 packets... (50)
Read 28692 packets (got 14183 RFP requests and 0 RCKs), sent 14181 packets... (49)
Read 28793 packets (got 14224 RFP requests and 0 RCKs), sent 14217 packets... (49)
Read 28894 packets (got 14446 RFP requests and 0 RCKs), sent 14298 packets... (50)
Read 28995 packets (got 14497 RFP requests and 0 RCKs), sent 14388 packets... (50)
Read 29096 packets (got 14538 RFP requests and 0 RCKs), sent 14388 packets... (50)
Read 29115 packets (got 14593 RFP requests and 0 RCKs), sent 14388 packets... (50)
Read 29216 packets (got 14954 RFP requests and 0 RCKs), sent 14418 packets... (49)
Read 29317 packets (got 14995 RFP requests and 0 RCKs), sent 14498 packets... (49)
Read 29418 packets (got 14955 RFP requests and 0 RCKs), sent 14515 packets... (50)
Read 29519 packets (got 14795 RFP requests and 0 RCKs), sent 14568 packets... (49)
Read 29620 packets (got 14736 RFP requests and 0 RCKs), sent 14539 packets... (50)
Read 29721 packets (got 14697 RFP requests and 0 RCKs), sent 14569 packets... (50)
Read 29822 packets (got 14658 RFP requests and 0 RCKs), sent 14718 packets... (49)
Read 29923 packets (got 14619 RFP requests and 0 RCKs), sent 14699 packets... (49)
Read 30024 packets (got 14580 RFP requests and 0 RCKs), sent 14691 packets... (50)
Read 30125 packets (got 15011 RFP requests and 0 RCKs), sent 14689 packets... (50)
Read 30226 packets (got 15052 RFP requests and 0 RCKs), sent 14700 packets... (49)
Read 30327 packets (got 15111 RFP requests and 0 RCKs), sent 14670 packets... (50)
Read 30428 packets (got 15152 RFP requests and 0 RCKs), sent 15019 packets... (49)
Read 30529 packets (got 15193 RFP requests and 0 RCKs), sent 15119 packets... (49)
Read 30630 packets (got 15233 RFP requests and 0 RCKs), sent 15119 packets... (49)
Read 30731 packets (got 15273 RFP requests and 0 RCKs), sent 15163 packets... (49)
Read 30832 packets (got 15314 RFP requests and 0 RCKs), sent 15207 packets... (50)
Read 30942 packets (got 15417 RFP requests and 0 RCKs), sent 15270 packets... (50)
Read 31041 packets (got 15458 RFP requests and 0 RCKs), sent 15319 packets... (49)
Read 31140 packets (got 15499 RFP requests and 0 RCKs), sent 15420 packets... (50)
Read 31245 packets (got 15958 RFP requests and 0 RCKs), sent 15470 packets... (49)
Read 31346 packets (got 16219 RFP requests and 0 RCKs), sent 15470 packets... (49)
Read 31447 packets (got 16260 RFP requests and 0 RCKs), sent 15470 packets... (49)
Read 31548 packets (got 15720 RFP requests and 0 RCKs), sent 15676 packets... (49)

Aircrack-ng 1.6

[00:00:00] Tested 19 keys (got 16134 IVs)

KB depth brk-(wizc)
0/ 1 12(598) 67(2298) 52(2154) 07(1914) 09(1048)
1/ 2 54(2352) 86(3592) 3(13480) 14(2024) 45(1988)
2/ 3 78(2016) 44(2148) 45(2148) 28(3982) 48(2092)
3/ 4 78(2016) 3(22272) 45(2148) 04(2148) 70(2092)
4/ 1 98(2380) 3(22272) 45(2148) 04(2148) 70(2092)

KEY FOUND | [12:34:56:78:99]
Decrypted correctly: 100%
[root@targetLinux01 /home/wifi/sta1]
```

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

```
*mon0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Exploiting Wireless Vulnerabilities (4e)          Lubuntu 2025-03-17 16:42:24
Isaiah Mosley

No. Time Source Destination Protocol Length Info
1 97 -1742243693.10 10.0.0.2 10.0.0.254 HTTP 1056 GET / HTTP/1.1
2 116 -1742243692.10 10.0.0.254 10.0.0.2 1056 HTTP/1.1 200 OK (text/html)

[Window size scaling factor: 512]
Checksum: 0x3043 [unverified]
[Checksum Status: Unverified]
[Urgent pointer: 0]
[Timestamps: 12.000ms, No-Operation (NOP), No-Operation (NOP), Timestamps]
> [SEQ/ACK analysis]
> [Timestamps]
> [TCP payload data (938 bytes)]
TCP segment data (938 bytes)
TCP segment data (938 bytes)
> [5 Resassembled TCP Segments (6730 bytes): #112(1448), #113(1448), #114(1448), #115(1448), #116(938)]
> [HTTP/1.1 Response Protocol]
> [HTTP/1.1 Response]
Date: Mon, 17 Mar 2025 21:10:27 GMT\r\n
Server: Apache/2.4.41 (Ubuntu)\r\n
Content-Type: text/html; charset=UTF-8\r\n
Content-Length: 6557\r\n
\r\n
HTTP response 1/1
[Tim since request: 1.291692516 seconds]
Request in Frame: 97
File URL: http://10.0.0.254/
File Data: 6557 bytes
Line-based Text data: text/html (212 lines)

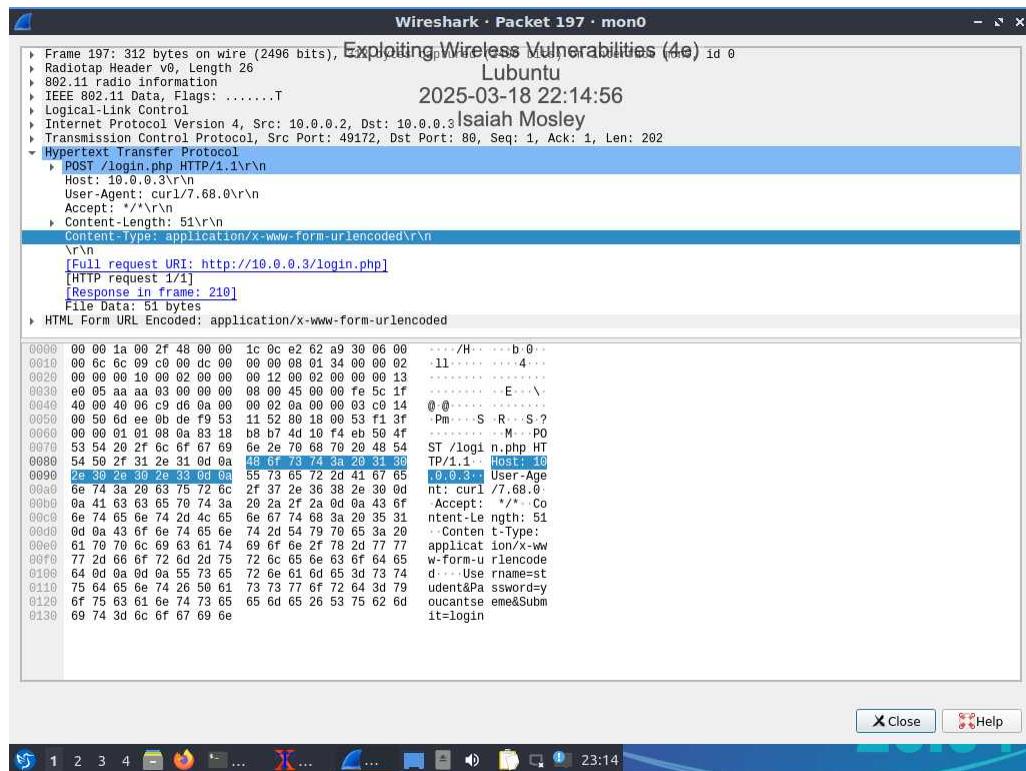
Frame (1056 bytes) Decrypted WEP data (998 bytes) Reassembled TCP (6730 bytes)
00000 aa aa 03 00 00 00 00 45 00 03 de ca 75 40 00 E .. uP
00010 40 06 3f 00 00 00 00 00 00 00 00 00 00 00 00 00 .. .. ..
00020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .. .. ..
00030 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .. .. ..
Frame (1056 bytes) Decrypted WEP data (998 bytes) Reassembled TCP (6730 bytes)
00000 aa aa 03 00 00 00 00 45 00 03 de ca 75 40 00 E .. uP
00010 40 06 3f 00 00 00 00 00 00 00 00 00 00 00 00 00 .. .. ..
00020 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .. .. ..
00030 01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .. .. ..

Packets: 409 - Displayed: 2 (0.5%) - Dropped: 0 (0.0%) Profile: Default
[root@targetLinux01 /home/wifi/sta1]
```

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.

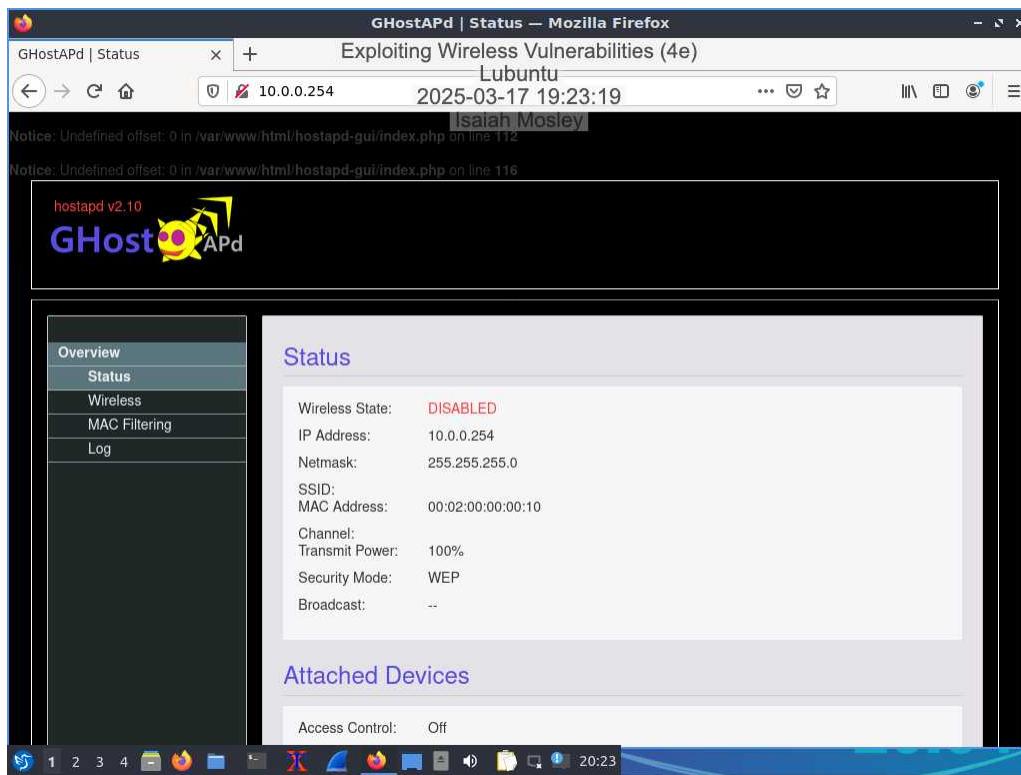


Part 2: Encrypt Wireless Traffic with WPA2

Exploiting Wireless Vulnerabilities (4e)

Ethical Hacking, Fourth Edition - Lab 07

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.**

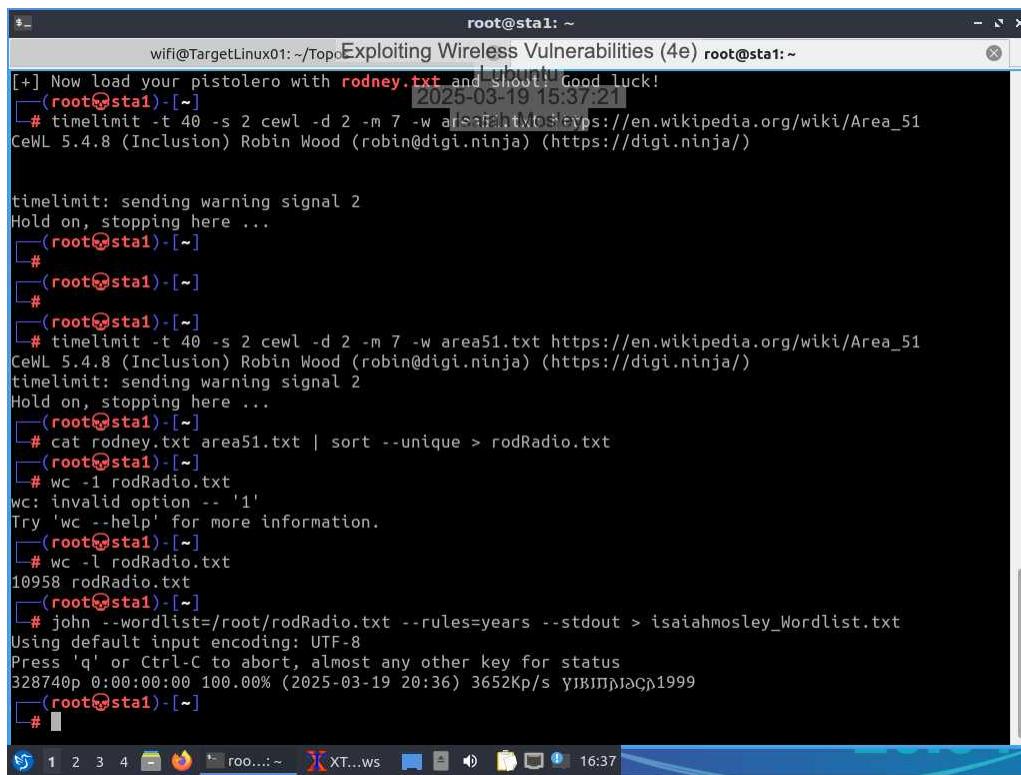
Incomplete

Part 3: Break WPA2 Encryption

Exploiting Wireless Vulnerabilities (4e)

Ethical Hacking, Fourth Edition - Lab 07

21. Make a screen capture showing the length of your new `yourname_Capture.txt` wordlist in the JtR output.



The screenshot shows a terminal window titled "root@sta1: ~" running on a Linux system. The window displays the following command-line session:

```
wifi@TargetLinux01:~/Top... Exploiting Wireless Vulnerabilities (4e) root@sta1:~  
[+] Now load your pistolero with rodney.txt and shoot! Good luck!  
[root@sta1]# 2025-03-19 15:37:21  
[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@digi.ninja) (https://digi.ninja/)  
  
timelimit: sending warning signal 2  
Hold on, stopping here ...  
[root@sta1]#  
[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@digi.ninja) (https://digi.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 -- '1'  
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 0:00:00 100.0% (2025-03-19 20:36) 3652Kp/s γΙΒΓΠΗΔΩΣ1999  
[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