

Wireless Access Exploitation

PCAP 1 (Easy)

This challenge evaluates the contestant's ability to crack WEP encryption given a packet capture. The [aircrack-ng](#) Linux tool can be used to solve this challenge.

Questions 1, 2, and 4 can be solved by simply running aircrack-ng on the packet capture. The summary lists the number of IVs that were found in the packet capture along with the WEP key. The key size can be determined by counting the number of bits in the key text (5 bytes * 8 bits per byte = 40 bits) and comparing that to the possible [WEP key sizes and configurations](#). Note: WEP keys are larger than the password input size.

aircrack-ng NCL-2015-WIFI1.pcap

```
Aircrack-ng 1.2 beta1
(00:00:03) Tested 134106 keys (got 14397 IVs)

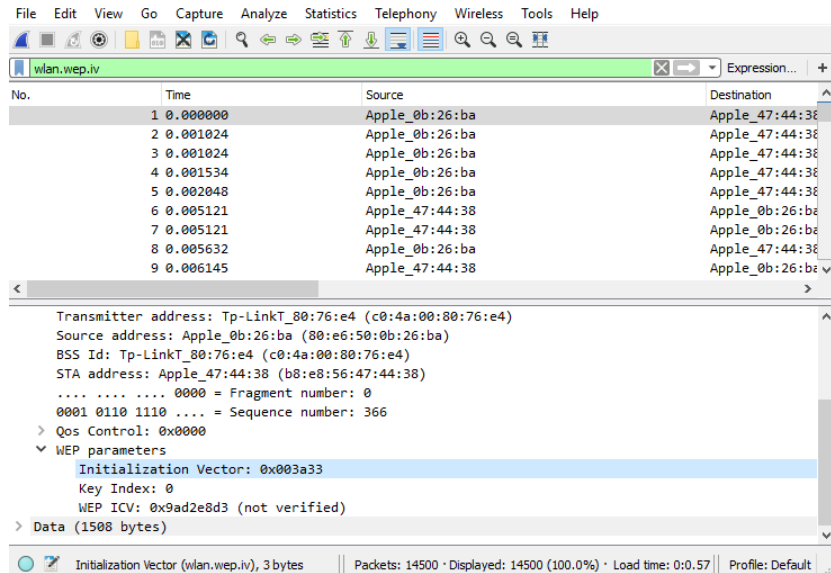
#B  depth  byte(vote)
0  1/ 3  A4(20736) 81(19968) DE(19200) 65(18944) F9(18944) 97(18688) 5D(18176) 94(18176) 16(17920) 4D(17920) 05(17920) FD(17920) 55(17664) BB(17664) C2(17664)
1  1/ 11  81(19200) 4C(19200) 08(18944) 47(18432) A6(18176) 8E(18176) 38(18176) 94(17664) 98(17664) 04(17664) 16(17408) 4B(17408) 4D(17408) 72(17408) 7A(17408)
2  2/ 26  53(18944) 73(18432) A8(18432) 0E(18432) C6(18432) 21(18432) 3B(18432) 5B(18432) AE(18176) 0D(18176) 46(18176) 7B(17920) 9E(17920) C9(17920) EE(17920)
3  4/ 9   84(18944) 10(18688) 2D(18432) 4B(18432) 08(18432) 19(18176) 4D(18176) 65(18176) 68(17920) 6C(17920) 2A(17664) 5E(17664) 92(17664) B7(17664) C9(17664)
4  12/ 18  15(17408) 34(17152) 46(17152) 51(17152) 7D(17152) FB(17152) 3B(16896) 81(16896) D6(16896) E1(16896) E2(16896) 05(16640) 37(16640) 5A(16640) 76(16640)

KEY FOUND! [ A4:B1:53:B4:CF ]
Decrypted correctly: 100%

root@kali:~/2015/wifi# aircrack-ng NCL-2015-WIFI1.pcap
```

Question 3 can be solved by viewing the packet capture in Wireshark and using the following filter:

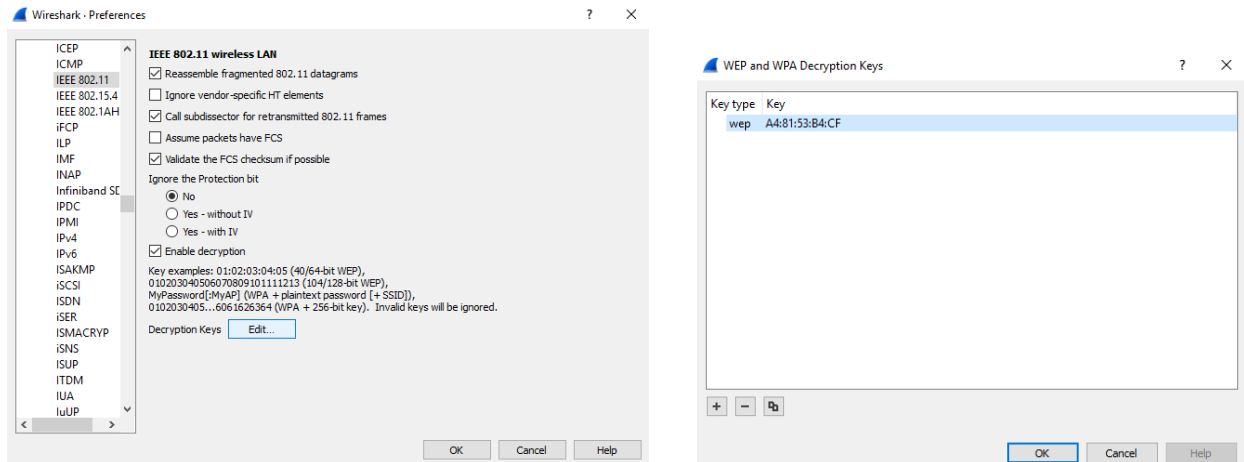
wlan.wep.iv





© 2017 Cyber Skyline. All Rights Reserved.
Unauthorized reproduction or distribution of this copyrighted work is illegal.

Question 6 can be solved by using the previously acquired WEP key to decrypt traffic in Wireshark. This can be done by selecting “Edit > Preferences > Protocols > IEEE 802.11” and then checking “Enable decryption” and adding the decryption key.



No.	Time	Source	Destination
1	0.000000	192.168.0.101	192.168.0.102
2	0.001024	192.168.0.101	192.168.0.102
3	0.001024	192.168.0.101	192.168.0.102
4	0.001534	192.168.0.101	192.168.0.102
5	0.002048	192.168.0.101	192.168.0.102
6	0.005121	192.168.0.102	192.168.0.101
7	0.005121	192.168.0.102	192.168.0.101
8	0.005632	192.168.0.101	192.168.0.102
9	0.006145	192.168.0.102	192.168.0.101
10	0.006654	192.168.0.101	192.168.0.102
11	0.006657	192.168.0.102	192.168.0.101
12	0.008704	192.168.0.101	192.168.0.102
13	0.008702	192.168.0.101	192.168.0.102
14	0.008702	192.168.0.101	192.168.0.102

> Logical-Link Control

> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 192.168.0.102

▼ Transmission Control Protocol, Src Port: 56985 (56985), Dst Port: 22 (22), Seq: 1, Ack: 1, Len: 1...

Source Port: 56985
Destination Port: 22
[Stream index: 0]
[TCP Segment Len: 1448]
Sequence number: 1 (relative sequence number)
[Next sequence number: 1449 (relative sequence number)]
Acknowledgment number: 1 (relative ack number)
Header Length: 32 bytes

> Flags: 0x010 (ACK)
Window size value: 4096
[Calculated window size: 4096]
[Window size scaling factor: -1 (unknown)]

> Checksum: 0x897b [validation disabled]
Urgent pointer: 0



© 2017 Cyber Skyline. All Rights Reserved.
Unauthorized reproduction or distribution of this copyrighted work is illegal.



© 2017 Cyber Skyline. All Rights Reserved.
Unauthorized reproduction or distribution of this copyrighted work is illegal.

Question	Answer
How many IVs are in the packet capture?	14337
What is the key size of the wireless network in bits?	64
What is the IV for the first packet in the capture (in hex)?	0x003a33
What is the WEP key?	A4:81:53:B4:CF
What is the TCP checksum of the first packet in the capture (in hex)?	0x897b

© 2017 Cyber Skyline



© 2017 Cyber Skyline. All Rights Reserved.
Unauthorized reproduction or distribution of this copyrighted work is illegal.