

[illegible]

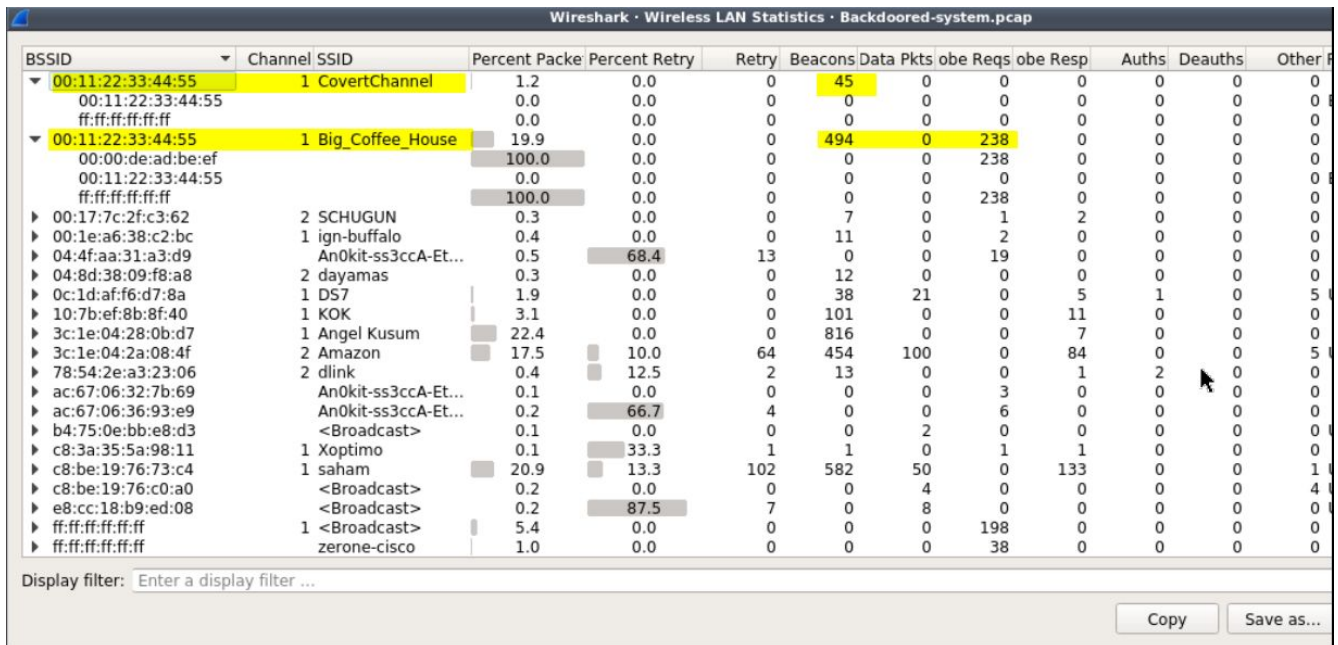
<b>Name</b>	Backdoored System
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=65">https://www.attackdefense.com/challengedetails?cid=65</a>
<b>Type</b>	Forensics : WiFi

**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.

**Question 1:** How is information is getting leaked out?

**Solution:**

The best way to start WiFi Forensics with Wireshark is to start with macro view. Check WLAN summary using Wireless > WLAN Traffic.



Wireshark · Wireless LAN Statistics · Backdoored-system.pcap

BSSID	Channel	SSID	Percent Packe	Percent Retry	Retry	Beacons	Data Pkts	obe Reqs	obe Resp	Auths	Deauths	Other
▼ 00:11:22:33:44:55	1	CovertChannel	1.2	0.0	0	45	0	0	0	0	0	0
00:11:22:33:44:55			0.0	0.0	0	0	0	0	0	0	0	0
ff:ff:ff:ff:ff:ff			0.0	0.0	0	0	0	0	0	0	0	0
▼ 00:11:22:33:44:55	1	Big_Coffee_House	19.9	0.0	0	494	0	238	0	0	0	0
00:00:de:ad:be:ef			100.0	0.0	0	0	0	238	0	0	0	0
00:11:22:33:44:55			0.0	0.0	0	0	0	0	0	0	0	0
ff:ff:ff:ff:ff:ff			100.0	0.0	0	0	0	238	0	0	0	0
▶ 00:17:7c:2f:c3:62	2	SCHUGUN	0.3	0.0	0	7	0	1	2	0	0	0
▶ 00:1e:a6:38:c2:bc	1	ign-buffalo	0.4	0.0	0	11	0	2	0	0	0	0
▶ 04:4f:aa:31:a3:d9		An0kit-ss3ccA-Et...	0.5	68.4	13	0	0	19	0	0	0	0
▶ 04:8d:38:09:f8:a8	2	dayamas	0.3	0.0	0	12	0	0	0	0	0	0
▶ 0c:1d:af:f6:d7:8a	1	DS7	1.9	0.0	0	38	21	0	5	1	0	5
▶ 10:7b:ef:8b:8f:40	1	KOK	3.1	0.0	0	101	0	0	11	0	0	0
▶ 3c:1e:04:28:0b:d7	1	Angel Kusum	22.4	0.0	0	816	0	0	7	0	0	0
▶ 3c:1e:04:2a:08:4f	2	Amazon	17.5	10.0	64	454	100	0	84	0	0	5
▶ 78:54:2e:a3:23:06	2	dlink	0.4	12.5	2	13	0	0	1	2	0	0
▶ ac:67:06:32:7b:69		An0kit-ss3ccA-Et...	0.1	0.0	0	0	0	3	0	0	0	0
▶ ac:67:06:36:93:e9		An0kit-ss3ccA-Et...	0.2	66.7	4	0	0	6	0	0	0	0
▶ b4:75:0e:bb:e8:d3		<Broadcast>	0.1	0.0	0	0	2	0	0	0	0	0
▶ c8:3a:35:5a:98:11	1	Xoptimo	0.1	33.3	1	1	0	1	1	0	0	0
▶ c8:be:19:76:73:c4	1	saham	20.9	13.3	102	582	50	0	133	0	0	1
▶ c8:be:19:76:c0:a0		<Broadcast>	0.2	0.0	0	0	4	0	0	0	0	4
▶ e8:cc:18:b9:ed:08		<Broadcast>	0.2	87.5	7	0	8	0	0	0	0	0
▶ ff:ff:ff:ff:ff:ff	1	<Broadcast>	5.4	0.0	0	0	0	198	0	0	0	0
▶ ff:ff:ff:ff:ff:ff		zerone-cisco	1.0	0.0	0	0	0	38	0	0	0	0

Display filter: Enter a display filter ...

Copy Save as...

The first two listings “CovertChannel” and “Big\_Coffee\_House” doesn’t have any data packets but only management packets (beacons and probe requests). This doesn’t happen in any normal network. It can happen if the network is not in use. But, it gives the investigator a reason to look into it. If we apply a filter to only check packets from “Big\_Coffee\_House”.

**Filter:** wlan contains Big\_Coffee\_House

The screenshot shows the Wireshark interface with the filter 'wlan contains Big\_Coffee\_House' applied. The packet list shows several beacon frames from source 'Cimsys\_33:44:55' to destination 'Broadcast' on protocol '802.11'. The packet details pane for the selected packet (No. 3404) shows the following structure:

- Tag: DS Parameter set: Current Channel: 1
  - Tag Number: DS Parameter set (3)
  - Tag length: 1
  - Current Channel: 1
- Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
  - Tag Number: Traffic Indication Map (TIM) (5)
  - Tag length: 4
  - DTIM count: 0
  - DTIM period: 1
  - Bitmap control: 0x00
  - Partial Virtual Bitmap: 00
- Tag: EDCA Parameter Set
  - Tag Number: EDCA Parameter Set (12)

The packet bytes pane shows the raw data of the beacon frame, including the frame control field, duration, address fields, and the management field (Type: 0, Subtype: 8).

Scrolling through the packets, we can observe some content being passed as the unknown IEs payload.

**Answer:** Backdoor is using beacon and probe request frames to get commands and send information out.

**Solution:**

The image shows a Wireshark packet capture of IEEE 802.11 Beacon frames. The top bar indicates the capture is on the 'wlan' interface, filtered by 'wlan contains Big\_Coffee\_House'. The packet list pane shows 11 packets, all of which are Beacon frames from source 'Cimsys\_33:44:55' to destination 'Broadcast' on the 802.11 protocol. The packet details pane for packet 11175 shows the RX flags as 0x0000, antenna signal as -8dBm, and antenna as 0. It also shows the 802.11 radio information and the IEEE 802.11 Beacon frame structure, including the Flags field (0x00000000) and the SSID field ('Big\_Coffee\_House'). The packet bytes pane shows the raw data of the beacon frame, including the frame control field, duration field, address fields, and the SSID field.

No.	Time	Source	Destination	Protocol	Length	Info
11136	278.429587	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=612, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11141	278.625357	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=614, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11142	278.727193	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=615, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11144	278.830927	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=616, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11146	278.934102	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=617, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11149	279.036214	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=618, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11150	279.139463	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=619, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11158	279.343323	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=621, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11161	279.445287	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=622, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11163	279.548528	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=623, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11167	279.648956	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=624, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11172	279.857112	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=626, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...
11175	279.956095	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=627, FN=0, Flags=.....C, BI=100, SSID=Big_Coffe...

▶ RX flags: 0x0000  
 Antenna signal: -8dBm  
 Antenna: 0  
 ▶ 802.11 radio information  
 ▶ IEEE 802.11 Beacon frame, Flags: .....C

Offset	Bytes	Hex	ASCII
0000	00 00 24 00 2f 40 00 a0	20 08 00 00 00 00 00 00	..\$. /@...
0010	74 fe 25 6a 84 9b 9b 36	10 02 6c 09 a0 00 f8 00	t%j...6..l...
0020	00 00 f8 00 80 00 00 00	ff ff ff ff ff ff 00 11	.....
0030	22 33 44 55 00 11 22 33	44 55 40 26 00 00 00 00	"3DU.. "3 DU@&...
0040	00 00 00 00 64 00 21 04	00 10 42 69 67 5f 43 6f	...d.!..Big_Co
0050	66 66 65 65 5f 48 6f 75	73 65 01 08 03 12 96 18	f fee_Hou se...
0060	24 30 48 60 03 01 01 05	04 00 01 00 00 0c 0a 54	\$0H'.....T
0070	72 61 64 65 50 72 69 63	65 04 20 45 fe	radePrice E:

- Attacker machine's MAC is 00:11:22:33:44:55 which seems fake.
- The RSSI of beacon frames is very high (in range of one digit i.e. -9 dBm). Hence, it is possible that attacker's transmitter is just outside the boundary, most probably just opposite to a wall from the sensor and can be high power and directional. So, it is possible that attacker is just above floor (above the ceiling on which the sensor is installed).



**Question 3:** What information has been exchanged?

**Solution:**

We have to check the payload of different packets, also you will notice the same payload/message in multiple packets.

### Payload 1

Backdoored-system.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan contains Big\_Coffee\_House

No.	Time	Source	Destination	Protocol	Length	Info
3417	105.831224	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=52, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3425	106.036158	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=54, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3430	106.240073	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=56, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3434	106.342315	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=57, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3437	106.453467	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=58, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3439	106.558042	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=59, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3442	106.646768	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=60, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3448	106.746153	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=61, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3454	106.849837	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=62, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3455	106.950798	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=63, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3461	107.052448	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=64, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3464	107.156945	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=65, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3466	107.258542	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=66, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3467	107.360069	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=67, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...
3486	107.563583	Cimsys_33:44:55	Broadcast	802.11	123	Beacon frame, SN=69, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_...

SSID: Big Coffee House

- Tag: Supported Rates 1.5, 9, 11(B), 12, 18, 24, 36, 48, [Mbit/sec]
- Tag Number: Supported Rates (1)
- Tag length: 8
- Supported Rates: 1.5 (0x03)

Offset	Hex	ASCII
0000	00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00	..\$/@.. .....
0010	34 6a ff cc 39 a5 a5 91 10 02 6c 09 a0 00 f9 00	4j..9... ..l.....
0020	00 00 f9 00 80 00 00 00 ff ff ff ff ff ff 00 11	..... .....
0030	22 33 44 55 00 11 22 33 44 55 e0 03 00 00 00 00	"3DU...3 DU.....
0040	00 00 00 00 64 00 21 04 00 10 42 69 67 5f 43 6f	....d!.. ..Big_Co
0050	66 66 65 65 5f 48 6f 75 73 65 01 08 03 12 96 18	ffee Hou se.....
0060	24 30 48 60 03 01 01 05 04 00 01 00 00 0c 08 53	\$0H'.....-S
0070	65 6e 64 44 61 74 61 89 9e fe 78	endData: ..x

## Payload 2

Backdoor-system.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Wlan contains Big\_Coffee\_House

No.	Time	Source	Destination	Protocol	Length	Info
3776	118.060136	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=62, FN=0, Flags=.....C, SSID=Big_Coffee_House
3781	118.163535	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=63, FN=0, Flags=.....C, SSID=Big_Coffee_House
3784	118.265833	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=64, FN=0, Flags=.....C, SSID=Big_Coffee_House
3786	118.365951	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=65, FN=0, Flags=.....C, SSID=Big_Coffee_House
3787	118.468365	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=66, FN=0, Flags=.....C, SSID=Big_Coffee_House
3791	118.567303	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=67, FN=0, Flags=.....C, SSID=Big_Coffee_House
3792	118.669328	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=68, FN=0, Flags=.....C, SSID=Big_Coffee_House
3793	118.770421	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=69, FN=0, Flags=.....C, SSID=Big_Coffee_House
3798	118.872193	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=70, FN=0, Flags=.....C, SSID=Big_Coffee_House
3800	118.973862	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=71, FN=0, Flags=.....C, SSID=Big_Coffee_House
3801	119.074631	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=72, FN=0, Flags=.....C, SSID=Big_Coffee_House
3803	119.176558	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=73, FN=0, Flags=.....C, SSID=Big_Coffee_House
3804	119.277562	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=74, FN=0, Flags=.....C, SSID=Big_Coffee_House
3805	119.380174	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=75, FN=0, Flags=.....C, SSID=Big_Coffee_House
3806	119.481928	Cetia_ad:be:ef	Broadcast	802.11	123	Probe Request, SN=76, FN=0, Flags=.....C, SSID=Big_Coffee_House

Tag: Supported Rates 1.5, 9, 11(B), 12, 18, 24, 36, 48, [Mbit/sec]  
 Tag Number: Supported Rates (1)  
 Tag length: 8  
 Supported Rates: 1.5 (0x03)  
 Supported Rates: 9 (0x12)

```

0000 00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00  ..$./@..  ....
0010 b2 64 97 e1 56 93 93 79 10 02 6c 09 a0 00 c8 00  ..d.V..y  ..l....
0020 00 00 c8 00 40 00 00 00 ff ff ff ff ff ff 00 00  ....@.....
0030 de ad be ef 00 11 22 33 44 55 b0 04 00 10 42 69  ......"3 DU...Bi
0040 67 5f 43 6f 66 66 65 65 5f 48 6f 75 73 65 01 08  ..g.Coffee_House..
0050 03 12 96 18 24 30 48 60 03 01 01 0c 1a 53 65 63  ....$OH'....Sec
0060 72 65 74 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 3a  ..ret info rmation:
0070 20 58 58 31 33 34 35 b4 46 e9 fa  ....XX1345: F..
  
```

### Payload 3

The image shows a Wireshark packet capture of Beacon frames. The packet list on the left shows packets 6573 to 6819, all from source Cimsys 33:44:55 to destination Broadcast. The selected packet (6819) is a Beacon frame with SSID: Big Coffee House. The packet details on the right show the following structure:

- Tag: Supported Rates 1.5, 9, 11(B), 12, 18, 24, 36, 48, [Mbit/sec]
- Tag Number: Supported Rates (1)
- Tag length: 8
- Supported Rates: 1.5 (0x03)
- Packet bytes: 0000 00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00 ..\$. /@. ....
- 0010 cf ca 12 8d 00 00 00 00 10 02 6c 09 a0 00 f8 00 .....l.....
- 0020 00 00 f8 00 00 00 00 00 ff ff ff ff ff ff 00 11 .....11.....
- 0030 22 33 44 55 00 11 22 33 44 55 a0 08 00 00 00 00 "3DU.. "3 DU.....
- 0040 00 00 00 00 64 00 21 04 00 10 42 69 67 5f 43 6f ....d..!..Big Co
- 0050 66 66 65 65 5f 48 6f 75 73 65 01 08 03 12 96 18 ffee Hou se.....
- 0060 24 30 48 60 03 01 01 05 04 00 01 00 00 0c 0d 43 \$0H' .....C
- 0070 72 69 74 69 63 61 6c 20 49 6e 66 6f e9 8e 22 41 critical Info: "A



## Payload 4

Backdoored-system.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan contains Big\_Coffee\_House

No.	Time	Source	Destination	Protocol	Length	Info
7367	199.345550	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=129, FN=0, Flags=.....C, SSID=Big_Coffee_House
7369	199.447523	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=130, FN=0, Flags=.....C, SSID=Big_Coffee_House
7377	199.550206	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=131, FN=0, Flags=.....C, SSID=Big_Coffee_House
7378	199.649331	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=132, FN=0, Flags=.....C, SSID=Big_Coffee_House
7379	199.751532	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=133, FN=0, Flags=.....C, SSID=Big_Coffee_House
7380	199.853489	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=134, FN=0, Flags=.....C, SSID=Big_Coffee_House
7382	199.953817	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=135, FN=0, Flags=.....C, SSID=Big_Coffee_House
7383	200.054254	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=136, FN=0, Flags=.....C, SSID=Big_Coffee_House
7384	200.169633	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=137, FN=0, Flags=.....C, SSID=Big_Coffee_House
7394	200.261246	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=138, FN=0, Flags=.....C, SSID=Big_Coffee_House
7397	200.360976	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=139, FN=0, Flags=.....C, SSID=Big_Coffee_House
7398	200.462210	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=140, FN=0, Flags=.....C, SSID=Big_Coffee_House
7399	200.564465	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=141, FN=0, Flags=.....C, SSID=Big_Coffee_House
7400	200.665153	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=142, FN=0, Flags=.....C, SSID=Big_Coffee_House
7408	201.157039	Cetia_ad:be:ef	Broadcast	802.11	129	Probe Request, SN=145, FN=0, Flags=.....C, SSID=Big_Coffee_House

▼ Tag: Supported Rates 1.5, 9, 11(B), 12, 18, 24, 36, 48, [Mbit/sec]  
 Tag Number: Supported Rates (1)  
 Tag length: 8  
 Supported Rates: 1.5 (0x03)  
 Supported Rates: 9 (0x12)

```

0000 00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00  ..$/@..
0010 15 a3 13 8d 00 00 00 00 10 02 6c 09 a0 00 c4 00  ..l...
0020 00 00 c4 00 40 00 00 00 ff ff ff ff ff ff 00 00  ....@...
0030 de ad be ef 00 11 22 33 44 55 10 09 00 10 42 69  ...."3 DU... Bi
0040 67 5f 43 6f 66 66 65 65 5f 48 6f 75 73 65 01 08  g_Coffee_House
0050 03 12 96 18 24 30 48 60 03 01 01 0c 20 43 72 69  ....$OH.... Cri
0060 74 69 63 61 6c 20 70 61 73 73 77 6f 72 64 3a 20  tical pa ssword:
0070 64 75 63 6b 73 5f 72 6f 63 6b 33 33 31 0e 33 b8  ducks_ro ck331 3
0080 97
  
```

## Payload 5

Backdoored-system.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan contains Big\_Coffee\_House

No.	Time	Source	Destination	Protocol	Length	Info
10233	250.425697	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=339, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10235	250.528759	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=340, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10239	250.630781	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=341, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10243	250.732190	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=342, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10248	250.835956	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=343, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10251	250.943599	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=344, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10253	251.045861	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=345, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10257	251.149602	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=346, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10263	251.255339	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=347, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10276	251.460787	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=349, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10280	251.564051	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=350, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10286	251.772085	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=352, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10288	251.873097	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=353, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10291	251.978022	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=354, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House
10294	252.080023	Cimsys_33:44:55	Broadcast	802.11	125	Beacon frame, SN=355, FN=0, Flags=.....C, BI=100, SSID=Big_Coffee_House

SSID: Big\_Coffee\_House

▼ Tag: Supported Rates 1.5, 9, 11(B), 12, 18, 24, 36, 48, [Mbit/sec]  
 Tag Number: Supported Rates (1)  
 Tag length: 8  
 Supported Rates: 1.5 (0x03)

```

0000 00 00 24 00 2f 40 00 a0 20 08 00 00 00 00 00 00  ..$/@..
0010 07 69 c0 69 84 9b 9b 36 10 02 6c 09 a0 00 f9 00  ..i.i...6..l...
0020 00 00 f9 00 80 00 00 00 ff ff ff ff ff ff 00 11  ....
0030 22 33 44 55 00 11 22 33 44 55 30 16 00 00 00 00  ....3DU...3 DU0...
0040 00 00 00 00 64 00 21 04 00 10 42 69 67 5f 43 6f  ....d.l...Big Co
0050 66 66 65 65 5f 48 6f 75 73 65 01 08 03 12 96 18  ffee Hou se...
0060 24 30 48 60 03 01 01 05 04 00 01 00 0c 0a 54  ....$OH....T
0070 72 61 64 65 50 72 69 63 65 01 77 b3 db  ....radePrIce e-w...
  
```

## Payload 6

Backdoored-system.pcap						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
wlan contains Big_Coffee_House						
No.	Time	Source	Destination	Protocol	Length	Info
11287	282.842190	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=260, FN=0, Flags=.....C, SSID=Big_Coffee_House
11288	282.948180	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=261, FN=0, Flags=.....C, SSID=Big_Coffee_House
11290	283.036793	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=262, FN=0, Flags=.....C, SSID=Big_Coffee_House
11292	283.138512	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=263, FN=0, Flags=.....C, SSID=Big_Coffee_House
11295	283.248588	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=264, FN=0, Flags=.....C, SSID=Big_Coffee_House
11297	283.442199	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=266, FN=0, Flags=.....C, SSID=Big_Coffee_House
11298	283.543582	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=267, FN=0, Flags=.....C, SSID=Big_Coffee_House
11301	283.644228	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=268, FN=0, Flags=.....C, SSID=Big_Coffee_House
11306	283.746536	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=269, FN=0, Flags=.....C, SSID=Big_Coffee_House
11312	283.846970	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=270, FN=0, Flags=.....C, SSID=Big_Coffee_House
11313	283.949884	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=271, FN=0, Flags=.....C, SSID=Big_Coffee_House
11333	284.052094	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=272, FN=0, Flags=.....C, SSID=Big_Coffee_House
11340	284.150370	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=273, FN=0, Flags=.....C, SSID=Big_Coffee_House
11349	284.252857	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=274, FN=0, Flags=.....C, SSID=Big_Coffee_House
11357	284.354541	Cetia_ad:be:ef	Broadcast	802.11	119	Probe Request, SN=275, FN=0, Flags=.....C, SSID=Big_Coffee_House
Tag: Supported Rates 1.5, 9, 11(B), 12, 18, 24, 36, 48, [Mbit/sec]						
Tag Number: Supported Rates (1)						
Tag length: 8						
Supported Rates: 1.5 (0x03)						
Supported Rates: 9 (0x12)						
0000	00 00 24 00 2f 40 00 a0	20 08 00 00 00 00 00 00	..\$/@.. .....			
0010	97 59 d4 69 84 9b 9b 36	10 02 6c 09 a0 00 d0 00	.Y.i...6 ..l.....			
0020	00 00 d0 00 40 00 00 00	ff ff ff ff ff ff 00 00	....@.... .....			
0030	de ad be ef 00 11 22 33	44 55 30 11 00 10 42 69	....."3 DU0...Bi			
0040	67 5f 43 6f 66 66 65 65	5f 48 6f 75 73 65 01 08	g_Coffee_House..			
0050	03 12 96 18 24 30 48 60	03 01 01 0c 16 54 72 61	....\$0H' .....Tra			
0060	64 65 20 50 72 69 63 65	3a 20 55 53 44 20 34 35	de Price : USD 45			
0070	30 30 30 36 fe 99 6b		0006--k			

**Answer:** We found 3 rounds of message exchange. Given below:

- Attacker -> Backdoored machine: SendData
- Backdoored machine -> Attacker: Secret information: XX1345
- Attacker -> Backdoored machine: Critical Info
- Backdoored machine -> Attacker: Critical password:ducks\_rock331
- Attacker -> Backdoored machine: TradePrice
- Backdoored machine -> Attacker: Trade Price : USD 45000