Wireless Penetration Testing – for realz

@rmellendick

rmellendick@gmail.com

DISCLAIMER

- This is provided for informational purposes only.
- It is illegal in most countries, especially the US, to connect, decrypt traffic, penetrate, or inject any Wi-Fi network other than your own or any network where you do not have explicit (ROE) permission given to you by the rightful owner.
- YOU are solely responsible for any and all of your own actions and assume the consequences of those actions.

Legal stuff

- Know the wiretap laws and do not violate them
  - Some states require that both parties consent to a phone call being recorded
  - Know the scanner laws for the state you are operating in, remember to check this before traveling out of state
- Make sure your activities are authorized in the written rules of engagement
- In most states it is legal to monitor any radio transmission as long as its not a telephone call or pager traffic
- Additional activities to avoid:
  - Jamming transmissions
  - Decoding pager traffic
  - Illegally transmitting

Why You Should Listen

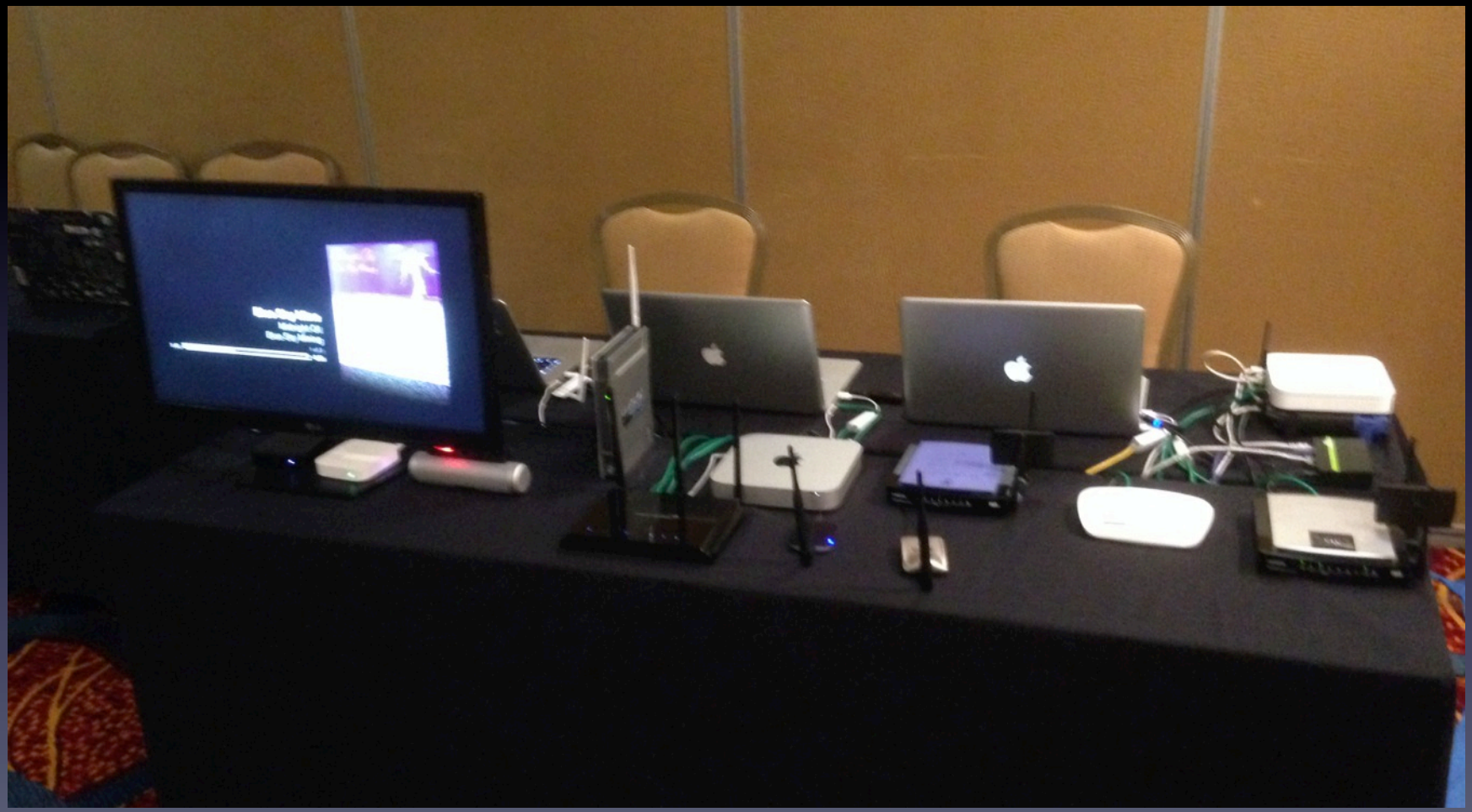
- You shouldn't
- I am old (in the wireless world)
  - Working with WiFi since 2002
- Total systems discovered
  - Rick > 43,000 wigle + 68,000 pentesting = badass
- First Wireless PenTest 2002/Most recent wireless pen test last week

DefCon 15 I

The Defcon15 Wireless Village entices you with THE TOWER of POWER !

DefCon 21 II

BSides DC III



BSides DE WCTF 2013

"RF Wars IV"

Methodology

- Develop a methodology make it repeatable
  - Scope work
    - Rules of engagement – **"get out of jail free"**
  - Enumeration/Assessment
  - Target information collection
    - SSIDs, ESSIDs & MACs
    - Modes of encryption
    - Parsing useful information from sites using EAP

Methodology

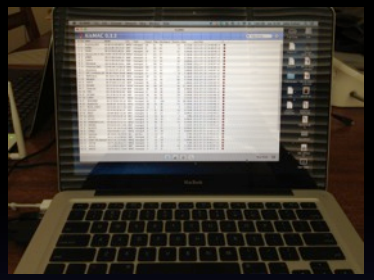
- Passive reconnaissance
- Exploitation
  - MiTM
  - Client side attacks
  - Cracking encryption
- Validation and Out-brief
  - Report
  - Why, Who, What, Where, How

Wireless Pentesting – What do I Need

- Platform Selection
- Selecting an Operating System
- Pentesting Software Choices
- Choosing Wireless Network Cards
  - 3 card setup vs. 2 card setup
- Deciding on an Antennas
- Always have the right tool for the job

Platform Selection

- Internet Access
  - Smart Phone with USB tether (WiFi/BT could be an issue)
- Laptop (MAC or PC)
  - Multi core processor
  - 8 GB ram or more* (16GB optimal)
  - Hard drive space for all necessary apps and VMs
    - SSD is optimal
  - Screen with space for multiple terminals
    - Use spaces
    - Use desktops
- External Radios/Antennas
  - Internal radios might not give the flexibility/capability
  - Built in antennas may not give flexibility needed
- Power Supply
    - Enough outlets to power all of your gear
      - Surge strip or splitter



Distributions

- OS X with Fusion
- Other Hosts with VM
- Windows (bare metal or VM)
- Pentoo (bare metal or VM)
  - Gentoo with Pentoo Overlay
- Kali (bare metal or VM)



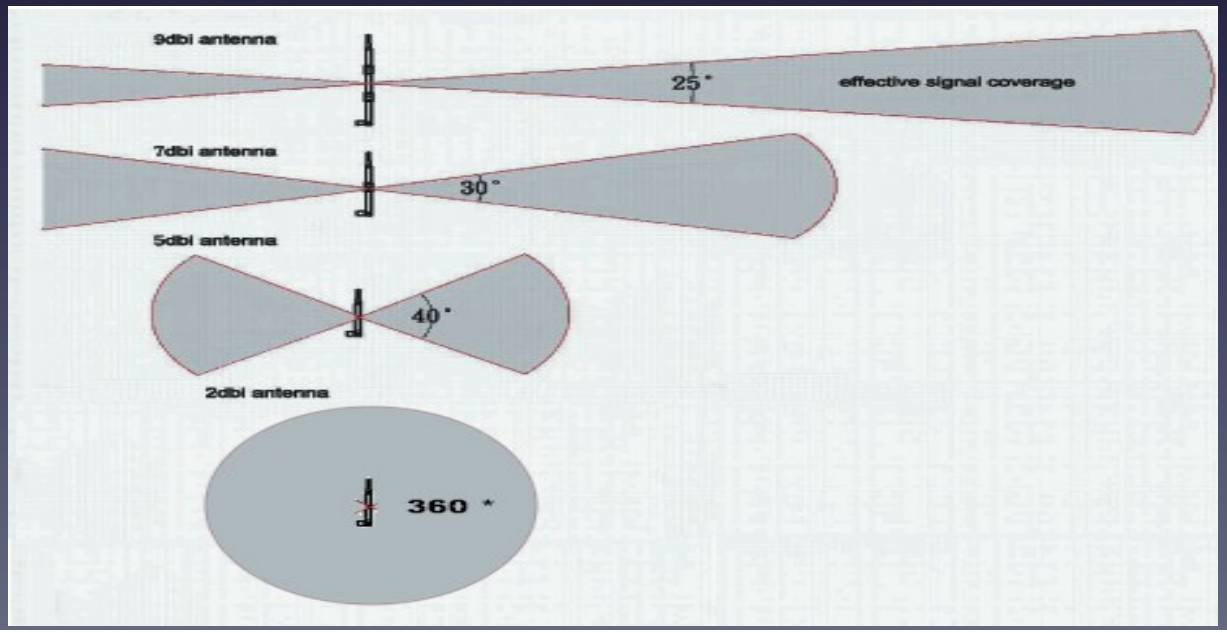


Tools

- Aircrack-NG
- Kismet-NG
- Airodump
- Wireshark
- TCPDump
- Nmap
- PGP
- Reaver
- Pyrit
- Wireshark
- OCLHashcat
- Wifite
- Fern-wifi-cracker
- Airdrop
- gqrx
- dsd
- multimon-ng
- smartnet-scanner
- gnuradi

Antennas

- Omnidirectional
  - 2, 5, 7 dBi
- Directional
  - Panel
  - Yagi



GPS Selection

- USB based
- Must be NMEA compliant
- Latest models
  - BU 353-S4 – 48 channels
  - Columbus V-800 – 66 channels
  - Add picture

Helpful Radios

- Alpha cards (B) (G) or (N) or (ABGN)
- Rokland N3 (BGN)
- Rosewill N600 UBE (ABGN)
- SR-71 (ABG)
- AirPcapNx (ABGN)
- WiSpy DBX (2.4 and 5Ghz)
- TP-Link TL-WN722N (BGN)
- EnGenius EUB 1200AC (ABGNAC)
- Ubertooth One (many uses)
- HackRF Jawbreaker (SDR)



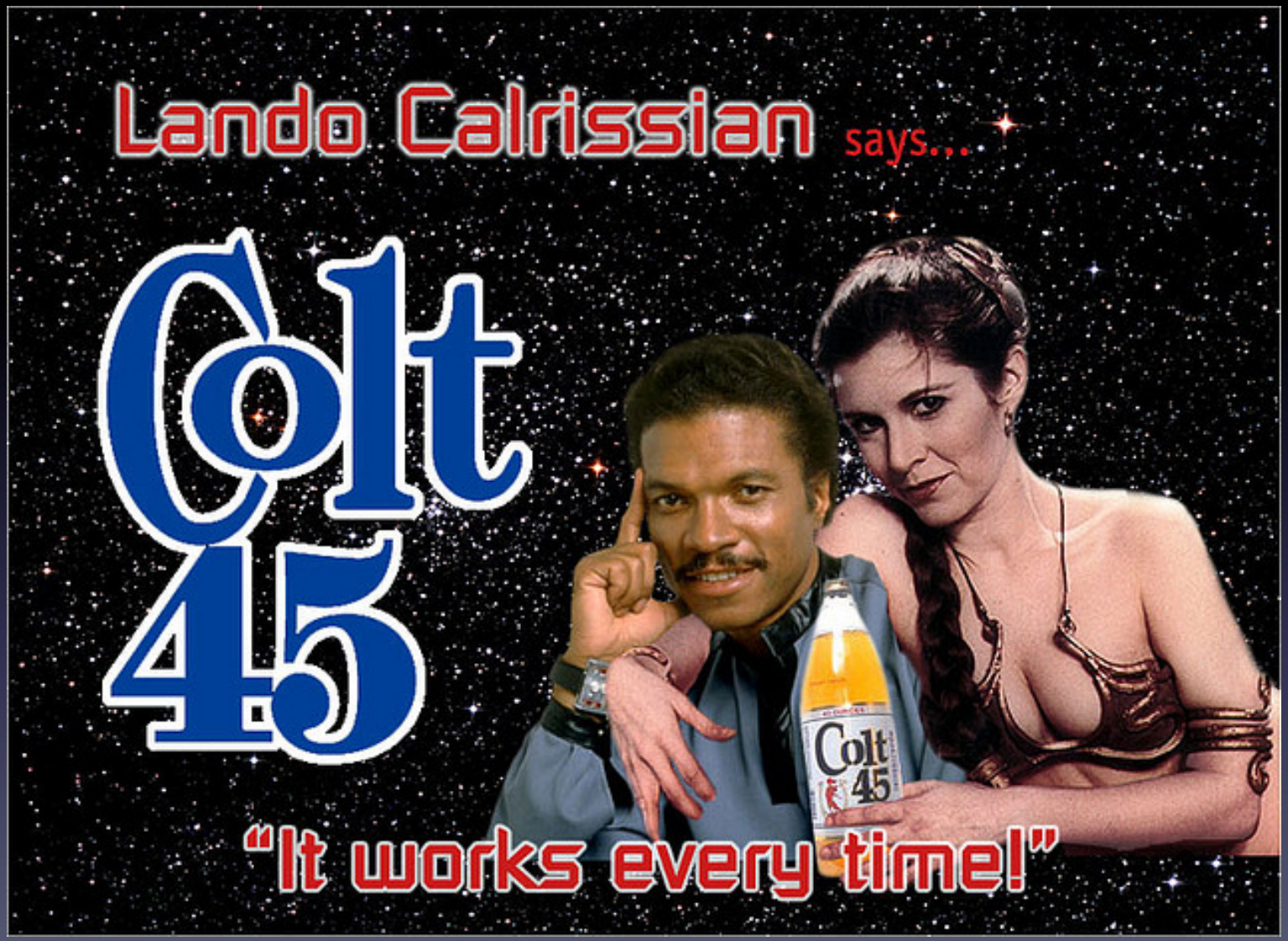






Testing Your Gear

- Have a repeatable process for validating antennas/setup
  - Hand testing on a fixed known AP
  - Automated testing Kismet (kismet script *shootout.rb*)
- Know how different cards, antennas, and combinations work with each platform
- Never be surprised by your equipment


Lando Calrissian says...
Colt 45
Colt 45
"It works every time!"

Wireless Pentesting Attacks

- MITM
  - Evil Access Point (Evil AP)
  - Jasager (WiFi Pineapple)
  - Karmetsploit
  - Attwifi (new attack)
  - PiWAT
  - PwnPlug
- Injection
- Bluetooth

Password Cracking

- Wireless Tools
  - Non-GUI
    - Aircrack-ng Suite
    - Pyrit
    - oclHashcat-plus/oclHashcat-lite
    - WEPCrack
  - GUI
    - Cain & Able
    - KisMac
    - hashcat-GUI

Pentest Tactics

- Figure out the clues, and think hard. The clues are always obscure and never direct, but will lead you to the answer.
- Make sure you have practiced with all setups in advance.
- Have a process or sequential processes to get through each challenge and follow that process!
- Take really good notes, either on paper or in a text file. I promise it will help.
- Learn about the person running the WCTF. This too will give a lot away.

PentestTactics

- airodump-ng --channel 1,6,11 --band abg wlanXmon --w channel_used --manufacturer
- Then get more and more specific
- Start with a 2Dbi antenna
- Move to a Panel
- Then lock in on your target BSSID

BeSides DE WCTF 2013

"RF Wars IV"

welcome to the challenge! Challenge 1 we will walk you through!

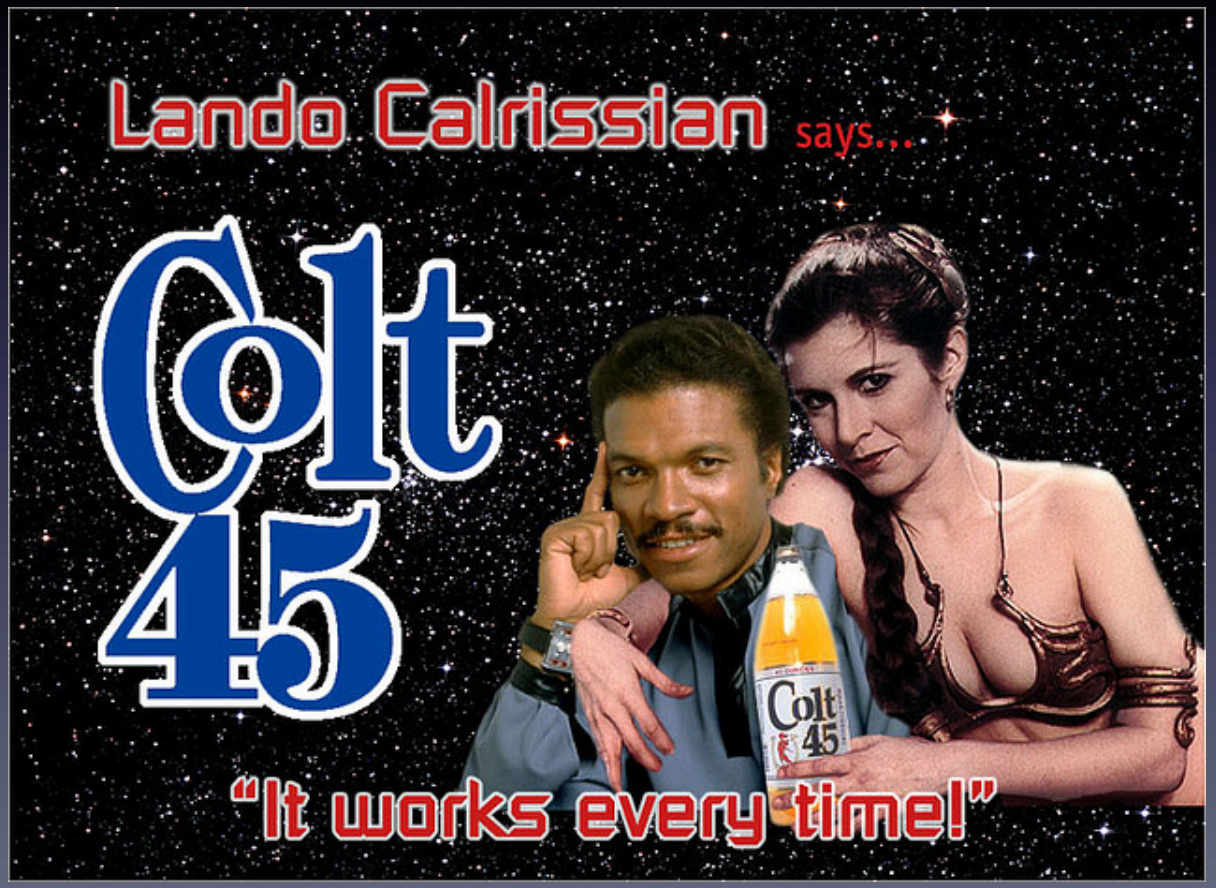
Challenge 2:
star wars ePisode iii: revenGe of the sith is different than the other five

Challenge 3: han WEpped as Princess leia sat in jail, alone and afraid

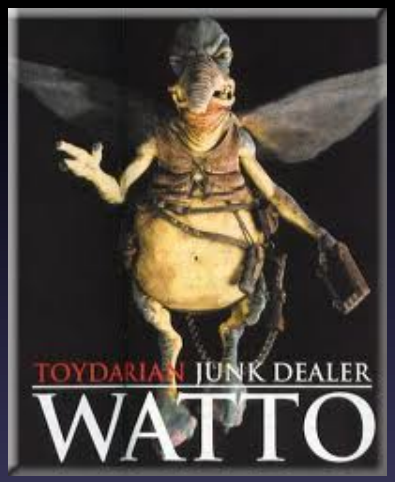
Challenge 4: mace Windu never Punched luke Skywalker but if he could have he would have

Challenge 4: R2-D2 said "beep, boop, beep, Ping as he flew through the air"

Challenge 6: "lAndo Calrissian was a colt 45 drinking mutha fuckah"



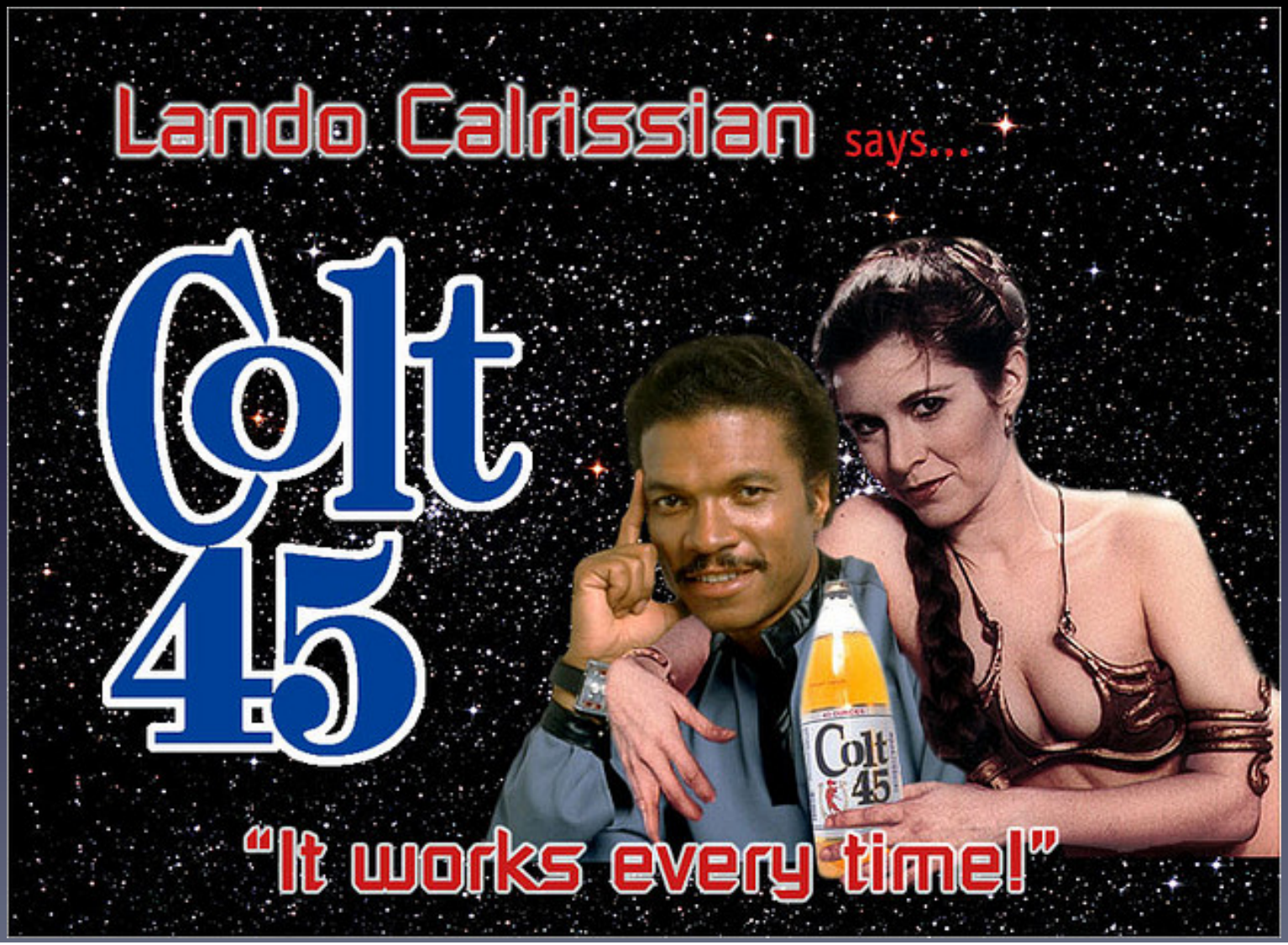
Challenge 7: this death star is protected by Watto, Padme', and chewbAccA and han can circle it in how many xxxxxxx"



Challenge 8: “Clone Captain reX”

Challenge 9A: “you Must uSe the Force to kill a Jedi with a Dual Homed light saber”

Challenge 9B: yes there is more… And we just had to reCycle this one more time, look for what is hiding and you will be silly PuTTY in her hands!



Special Thanks

ZC

Anch

Marauder

Terrible

DaKahuna

Thex1le (textile)

Questions

@Rmellendick

rmellendick@gmail.com