DEFCON 24 WCTF

Friday, August 4, 2016

Legal Issues: KNOW BEFORE YOU DO

- Consult a lawyer if you have questions. We are not lawyers, and you probably aren't either (www.fcc.gov)!
- DON'T frequency jam
  - Protocol jamming is another story
- If it feels wrong, it probably is
- We authorize you to attack this network, this is a secure network by playing and attaching to the network you consent to whatever happens… Play for fun and at your own risk!

What Is the WCTF?

- You will be using tools like the RTL-SDR, HackRF, BladeRF, your cell phone, and various A, B, G, N, and AC radios to find, identify, decode, and decrypt wireless signals.
- The WCTF can be played with a little knowledge, a pen tester's capability, $40 worth of equipment, or $4000 worth of equipment, but the key is to read the clues and determine the goal of each challenge.
- There will be clues everywhere, and we will provide periodic updates so make sure you pay attention to what's happening at the WCTF desk, on Twitter, the interwebz, etc. If you have a question - ASK, and we will determine if we will answer.
- To score you will need to submit flags which will range from transmissions in the spectrum, pass-phrases used to gain access to wireless access points, to files located on servers. Once you capture the flag, submit it right away because some will be timed challenges and others will be negative points. Offense and defense are fully in play by the participants, the WCTF organizers, and the Con itself.

What Is the WCTF?

- Resources
  - http://sdr.ninja
  - http://wctf.us
  - @wctf_us
  - http://www.sigidwiki.com/wiki/
- Gear
  - This is the gear talk if you are interested
  - http://wctf.us/docs/BsidesDC_2015__inbrief.pptx

Wireless Capture the Flag (WCTF)

- There are officially over 100 flags for challenges this year, and 25 additional flags that are available for different acts of hackery.
- Challenges are all RF 72 MHz – 5.8GHz

Challenges

@wctf_US
http://wctf.us
http://Sdr.ninja

Budget Your Time

- Challenges do not have to be solved in order
- Difficulty ranges from easy to insane
- Pay attention to details
- Don’t dwell on the problem
- Ask questions, learn things, have fun
- Check Twitter regularly

@wctf_us

Mobile Challenges

@wctf_US
http://wctf.us
http://Sdr.ninja

WiFi - Fox and Hound (1 per day)

ESSID and MAC address will be announced at 1130 on Friday and 1030 Saturday and 0900 on Sunday via Twitter

You must bring back the Fox to get the flags, on the day it was released

@wctf_us

750 points available per fox

WiFi - Hide and Seek (1 per day)

ESSID and MAC address will be announced at 1130 on Friday and 1030 Saturday and 0900 on Sunday via Twitter

You must bring back evidence of the hidden agent's location

a picture of the device, or room, or booth that it is located in to get the flags

@wctf_us

750 points per hidden agent

Blue Tooth - Fox and Hound 1

MAC address will be announced at 1130 on Friday and Saturday and 0900 on Sunday via Twitter

You must bring back the Fox to get the flags on the day it was released

@wctf_us

350 points per fox per day

Blue Tooth - Fox and Hound 2

MAC address will be announced at 1130 on Friday and Saturday and 0900 on Sunday via Twitter

You must bring back the Fox to get the flags on the day it was released

@wctf_us

500 points per fox per day

Blue Tooth - Fox and Hound 3

MAC address will be announced at 1130 on Friday and Saturday and 0900 on Sunday via Twitter

You must bring back the Fox to get the flags on the day it was released

@wctf_us

750 points per fox per day

Blue Tooth - Hide and Seek (1 per day)

MAC address will be announced at 1130 on Friday and Saturday and 0900 on Sunday via Twitter

You must bring back evidence of the hidden agent's location (a picture of the device, or room, or booth that it is located in to get the flags).

@wctf_us

750 points per hidden agent

SDR - Fox and Hound (1 per day)

MAC address will be announced at 1130 on Friday and Saturday and 0900 on Sunday via Twitter

Different Frequency each time!

You must bring back the Fox to get the flags on the day it was released

@wctf_us

750 points per fox per day

SDR- Duck Hunt

In the SDR Duck Hunt, a player not only has to find the transmitter, but also exercise knowledge of radio communications to transmit back to then receive the points.

http://sdr.ninja/training-events/sdr-dunk-hunt/

50 points per duck; one duck per hour

If you were to want to shoot aimlessly into the sky, a command such as the below would achieve that if you were using a RaspberryPi to transmit with PiFM:

```
#!/bin/sh
while true ; do echo "bang" | minimodem --tx -f -8 1200 -f /home/pi/bang.wav && /home/pi/pifm
/home/pi/sentence.wav 80.0 48000 ; sleep 4;done
```

Room Challenges

@wctf_US
http://wctf.us
http://Sdr.ninja

Test Flag WCTF_00

Welcome to WCTF! This is your first challenge. Attach to the rebel base wireless to confirm you can connect, then submit the WPA key to confirm you can use the scoring engine for +10 points.

Gone_Rogue

WCTF_01

WEP

Enter me to get to the SCADA challenges

50 Points

WCTF_02

WEP but like Alderaan

75 Points

WCTF_03

WEP AP like Anakin’s legs

100 Points

WCTF_04

Easy WPA

50 Points

WCTF_05

WPA

75 Points

WCTF_06

WPA at Starbuck's

150 Points

WCTF_07

WPA leave your deauths at home

200 Points

WCTF_08

WPA like Howie Mandel

200 Points

WCTF_09

Secure WPA

350 Points

SDR Drinking Game

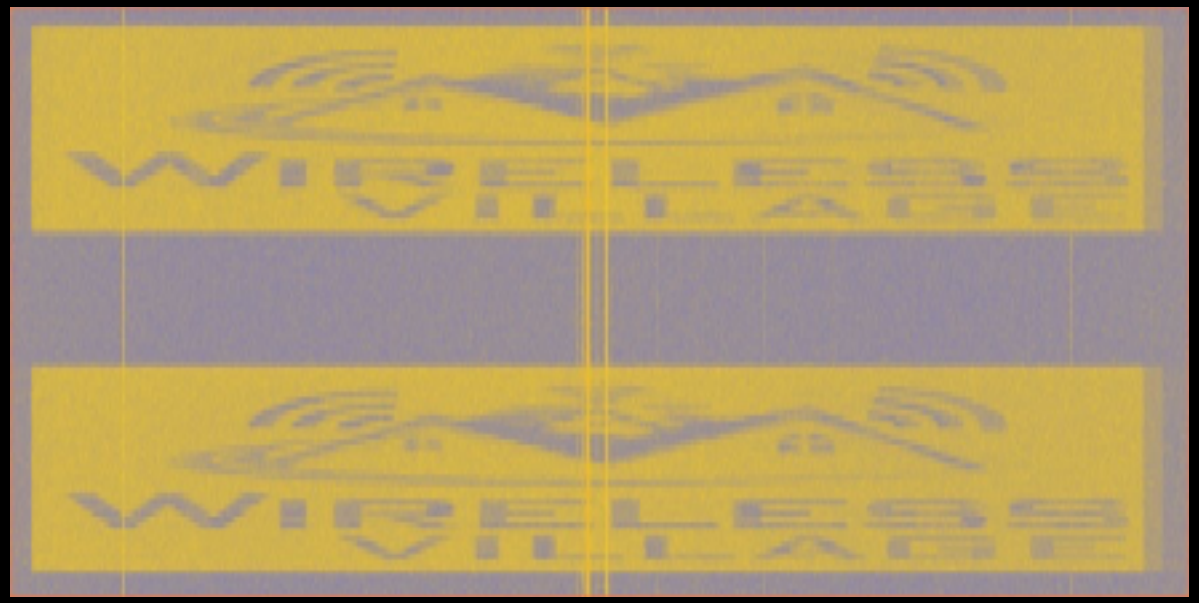
Saturday at 1500

Base line your system now get to know the spectrum in the area, the frequency ranges for the game will be in the useable range of the RTL-SDR

Find the frequency faster than everyone else, get the points and flip a coin, either you drink or everyone else drinks

50 Points per frequency

SDR Drinking Game



50 Points per frequency

SDR Shootout

Sunday at 1000

Two Players place laptops at opposite ends of room with no apps open, password locked
Players start back to back, and go to their laptops
First player to shock the other wins!
No repeat players

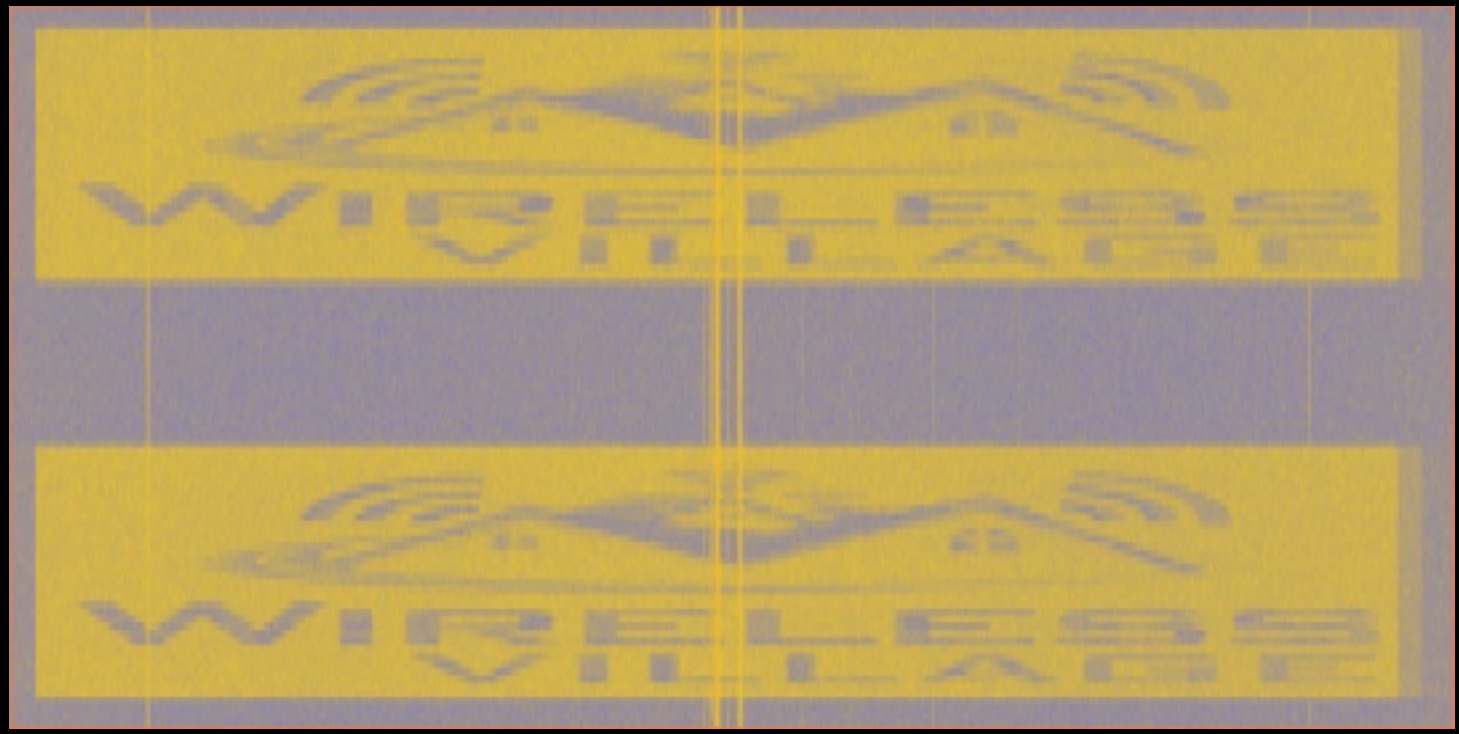
100 Points per round

SDR Challenge Frequencies

Instead of giving you the frequencies,
Look for the RF spray paint.

SDR Challenge Frequencies

Reference frequency for the con is 900MHz



SDR_01

Video Killed the Radio Star

5 flags

50 - 100 Points

SDR_02

Spy’s Like Us!

4 flags

50 - 200 Points

SDR_03

If bees couldn’t zag.

4 flags

50 - 100 Points

SDR_04

HAMR TIME

5 flags

50 - 150 Points

SDR_05

/dev/random

5 flags

50 - 250 Points

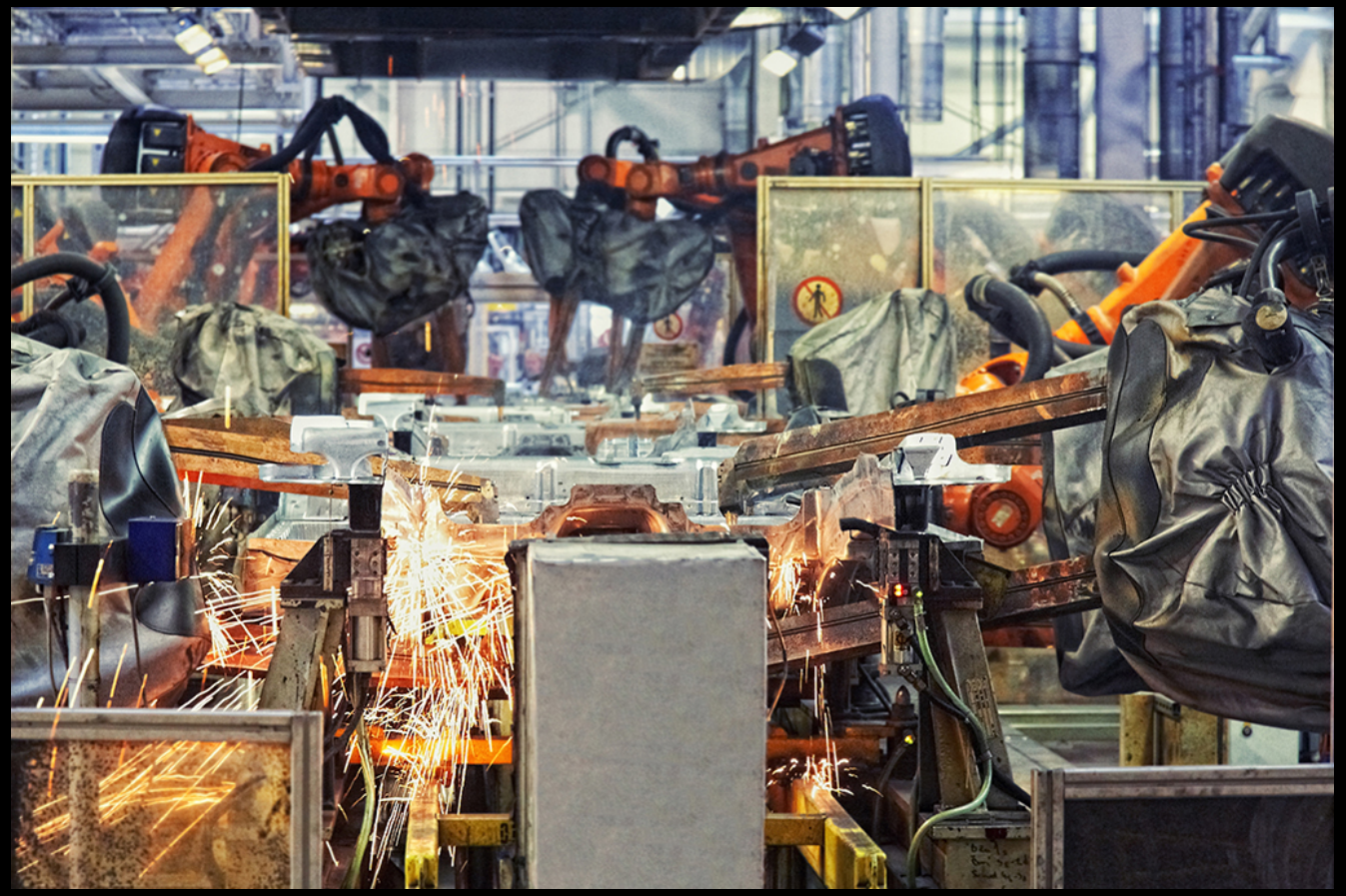
Holy Shit SCADA Challenges!!!!!!

@wctf_US

http://wctf.us

http://Sdr.ninja

Holy Shit SCADA Challenges!!!!!!



SCADA_01

What's the Switch IP

100 Points

SCADA_02

PLC IP

100 Points

SCADA_03

Switch Password

100 Points

SCADA_04

I/O Password

100 Points

SCADA_05

File in I/O filesystem (flag.txt)

100 Points

SCADA_06

I/O Byte Pattern for the button1 (hex)

50 Points

SCADA_07

I/O Byte Pattern for the button2 (hex)

50 Points

SCADA_08

I/O Byte Pattern for the button3 (hex)

50 Points

SCADA_09

I/O Byte Pattern for the button4 (hex)

50 Points

SCADA_10

I/O Byte Pattern for the button5 (hex)

50 Points

SCADA_11

I/O Byte Pattern for the light1 (hex)

50 Points

SCADA_12

I/O Byte Pattern for the light2 (hex)

50 Points

SCADA_13

I/O Byte Pattern for the light3 (hex)

50 Points

SCADA_14

I/O Byte Pattern for the light4 (hex)

50 Points

SCADA_15

I/O Byte Pattern for the light5 (hex)

50 Points

SCADA_16

SHA1 Hash for user.dat file for PLC (lower case)

200 Points

Final Surprise

13 years ago there was the Worldwide Wireless War Drive, we are bringing it back

Rules are simple, WarDrive, WarWalk, or War”anything”

Turn in your .netxml from kismet or airodump-ng by 0930 Sunday (NO PCAPS WILL BE ACCEPTED) remember this is circuit 9!, thanks California!!

Final Surprise

Points are as follows:

.065 points per unique BSSID (validated by us)
.13 points per unique BSSID (validated by us) with GPS

We reserve the right to refuse any submission we deem to be fake, or otherwise not genuine. This contest runs from NOW until 0929 Sunday.

Final Surprise

Submit by .xz tarball to:

wirelessvillageandctf@gmail.com

By 0929 Sunday 07-Aug-2016

Final Word

We play too, this is fun for all of us, have fun enjoy, and the rules are that there are no rules!

And don’t get arrested, leave the casino alone, this is for your own good, those rooms in the basement exist

Questions

@wctf_US

http://wctf.us

http://sdr.ninja