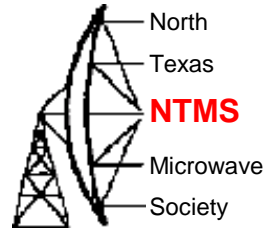North
Texas
NTMS
Microwave
Society

Universal Radio Hacker

NTMS meeting
March 8, 2025
KM5PO

What is it?

- Tool to receive, analyze and retransmit signal data
- Supports most current SDR Radios
- RTL-SDR (RX only), HackRF, Pluto, Airspy
- Runs on Linux, MacOS, Windows
- Automatic demodulation
  - Modulation identification
  - Customizable decode parameters
- Protocol reverse-engineering tools
- Simulation environment for stateful attacks
- https://github.com/jopohl/urh?tab=readme-ov-file

Ethical Hacking
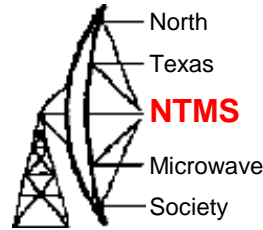
- A new industry of Systems Security improvement practice
- Identifying security weakness and providing remediation
- Involves more systems than RF based signaling
- Bug Bounty Hunter
- Comprehensive RF hacking tutorial available here:
- https://youtu.be/3Y4ve2O5jzk?si=yw4XF78oDUtVBTgN

Ethical Hacking
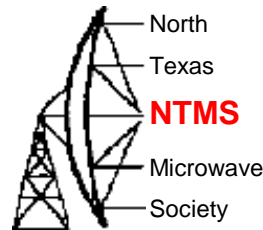
HackRF One PortaPack: A Complete RF Hacking Toolbox

4.0 ★ (42 ratings) 311 students

Hacking Toolbox

Unlocking the Power of HackRF One PortaPack: Strategies for Penetration Testing and Security Enhancement

4.0 ★★★★☆ (42 ratings) 311 students

Created by Arsalan Saleem, Secure Techware

📅 Last updated 2/2025   🌐 English   💬 English [Auto]

$59.99

Add to cart

Buy now

30-Day Money-Back Guarantee

This course includes:

▶ 2.5 hours on-demand video
⤓ 6 downloadable resources
📱 Access on mobile and TV
∞ Full lifetime access
🏆 Certificate of completion

Share   Gift this course   Apply Coupon

Preview this course

What you'll learn

✓ Assemble & configure HackRF One PortaPack H2 for security testing.

✓ Uncover device frequencies: launch replay attacks, jam signals.

✓ Become a communication expert: receive & transmit diverse signals (FM, POCSAG, ADS-B, APRS).

✓ Unlock Raspberry Pi's power: integrate for advanced signal transmission.

✓ Develop a comprehensive skillset for advanced penetration testing.

✓ Master Mayhem firmware: navigate Rx/Tx menus, optimize antennas.

✓ Advanced techniques: explore GPS spoofing and AI-powered frequency discovery.

✓ Hack FPV drone camera feeds.

✓ Learn safe practices for working with Software-Defined Radio (SDR) equipment.

✓ Gain confidence using HackRF One PortaPack H2 for security assessments.
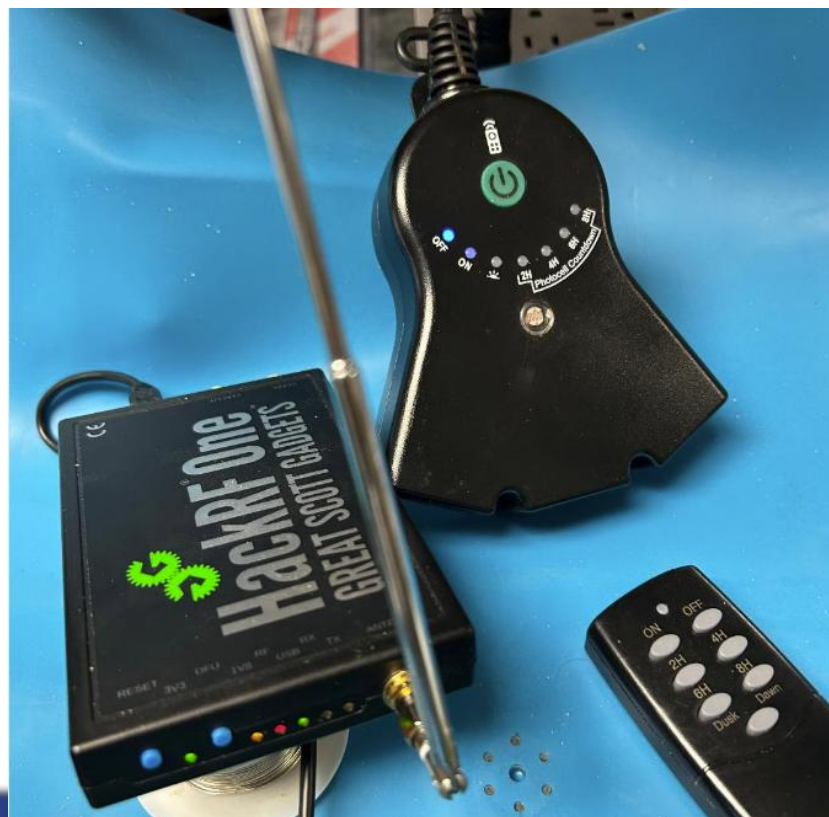
Training 2 or more people?

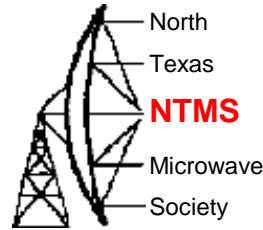Get your team access to 27,000+ top Udemy

Devices tested
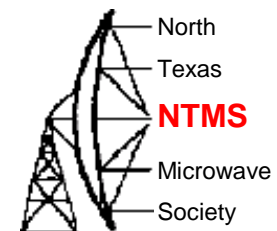
Devices tested

- Remote controlled outdoor power distro
 - So we can "light up" the deer herd!

Replay steps with Universal Radio Hacker

North
Texas
NTMS
Microwave
Society

- Identify the transmitted signal of the device (locate frequency)
    - Using Spectrum Analyzer
- Record the transmitted signal
    - Send commands over the air or intercept
- Trim modulated signal (optional)
- Transmit trimmed modulated signal through SDR Radio
- Optionally analyze modulation

North
Texas
NTMS
Microwave
Society

Replay demo
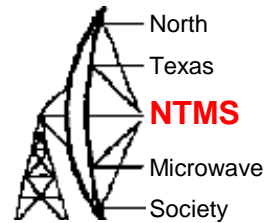
Open a file or record a new signal using the **File menu** to get started.

Questions?