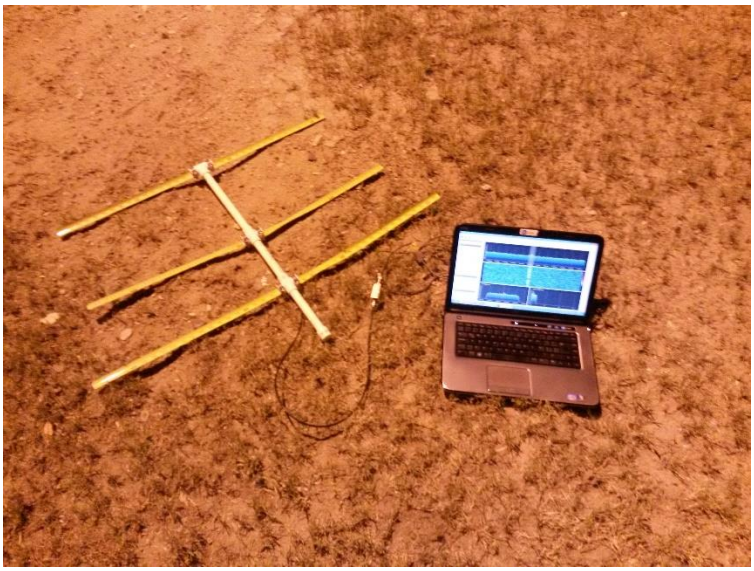
Explotación práctica de señales de radio con Software Defined Radio



Category

talk

Presentation abstract

¿Sabías que es posible recibir señales de radio de aviones, barcos y hasta satélites de una manera fácil y económica? Software Defined Radio tendrá un papel clave en seguridad en telecomunicaciones inalámbricas como una amenaza y será una herramienta más que los pentesters deberían conocer. Anteriormente se utilizaba Software Defined Radio en los círculos académicos para hacer investigación en tecnologías inalámbricas, pero dado su costo, software inmaduro y conocimiento requerido no resultaba práctico para profesionales de la seguridad. Esto está cambiando y proyectos como el RTL SDR y HackRF nos permite llevar ataques prácticos y hacer investigación en protocolos inalámbricos de una forma más accesible.

Additional details about your presentation (Supporting details, 0-day specifics, etc)

- La importancia de la seguridad en señales de radio
- Fuentes principales de inseguridad
    - Mal diseño de protocolos
    - Dificultad de realizar pruebas (costo y tiempo)
- Software Defined Radio
    - ¿Qué es SDR?
    - Algunos sistemas de telecomunicaciones vulnerables (incluye aviones)
    - ¿Porque hasta ahora?
    - Demo 1: Radar de aviones casero
    - Demo 2: Interceptor de mensajes SMS
    - Demo 3: Sintonizando bases aéreas militares
    - Demo 4: Recibiendo otras señales de interés aeronáuticas
    - ¿Cómo puedo empezar a sintonizar frecuencias en este momento? (Buscaremos señales disponibles en Buenos Aires como ejemplo)
    - Demo 5: Recuperando y tomando control de un satélite con permiso de la NASA

- Demo 6: Modificando la cola en un restaurante
- SIGINT like the NSA
- El futuro de SDR y cómo puedes ser parte de él

What do you hope attendees will gain from the presentation?

Quiero que los asistentes conozcan algunas de las cosas que se podrían hacer con Software Defined Radio (tanto la amenaza que representa y el potencial como profesionales de la seguridad informática), y que además es un campo muy nuevo por explorar y motivarlos a que se interesen por conocer más e experimentar más sobre este tema.

Describe three reason why this is a quality ekoparty presentation

- Software Defined Radio va a tener un gran crecimiento en los próximos años y es importante que los penetration testers conozcan que esto existe.

- Generalmente las presentaciones de este tema vienen de gente con mucho entrenamiento en ingeniería electrónica. (Sin mencionar que es fuera de Latinoamérica) Tengo experiencia como pentester y aficionado a la radio de muchos años por lo cual puedo hacer una presentación que sea útil a profesionales de seguridad.

- Me apasiona el tema y transmitiré eso a los asistentes.

Presentation time

50m

Check any that apply

- [ ] Has this presentation been previously presented? if YES, where:
- [ ] Are you releasing a new tool(s)?
- [ ] Are you releasing a new vulnerability/0-day?
- [x] Is there a live demonstration?
- [ ] Is there audience participation?
- [ ] Are you or your company paying your expenses (flight, hotel, etc)?
- [x] Are you willing to make a workshop?