Charla de Seguridad Digital para el Mundo Maker

"Entender los riesgos para protegerse sin paranoia"

[DrYouu]

Contents

1 Introducción: Tecnología y Seguridad en el Mundo Maker

En el ecosistema maker convergen creatividad, hardware abierto, protocolos diversos y, en muchas ocasiones, ausencia de controles de seguridad básicos. Esto abre puertas tanto a la innovación como a la exposición involuntaria a riesgos digitales con impacto físico.

- ¿Por qué importa la seguridad digital hoy?
- El perfil maker: creatividad, experimentación, exposición.
- Riesgos inadvertidos por exceso de confianza en la tecnología.

2 El Flipper Zero: El Cuchillo Suizo del Pentesting Personal

2.1 ¿Qué es el Flipper Zero?

Dispositivo multifunción de pentesting orientado inicialmente a investigadores de seguridad. Actualmente es ampliamente accesible para cualquier persona interesada.

2.2 Funciones principales

- Sub-GHz (mandos, garajes, sensores)
- RFID (tarjetas de acceso)
- Infrared (controles remotos)
- GPIO hacking (hardware hacking)
- USB HID (BadUSB)
- Bluetooth/BLE

2.3 Add-ons y expansión

- Wi-Fi Devboard
- Antenas externas
- Scripts y firmwares alternativos

2.4 Desde el punto de vista de la víctima

- Robo de señales
- Clonación de accesos
- Spoofing y suplantación
- Interacciones físicas peligrosas

3 Amenazas Digitales con Impacto en el Mundo Físico

- Cerraduras electrónicas
- Controles de acceso a edificios
- Garajes, barreras y portones
- Dispositivos DIY sin protocolos seguros

4 Hackeo Social: Atacar a la Persona

4.1 Ingeniería social aplicada al mundo maker

- Suplantación de roles
- Observación de rutinas
- Interacción física encubierta

4.2 Ataques combinados

- Evil Twin Wi-Fi
- HID scripts en eventos presenciales
- Escucha pasiva de frecuencias RFID

5 Cómo Protegerse sin Paranoia

5.1 Prácticas físicas

- Fundas Faraday
- Gestión de dispositivos de acceso
- Minimización de señales radiadas

5.2 Prácticas digitales

- Firmware actualizado
- Autenticación multifactor
- Desactivar interfaces no usadas

6 Ética Hacker y Cultura del Pentesting

- Diferenciar hacker de criminal
- Principios de divulgación responsable
- Ética en el uso de herramientas de pentesting

7 Comparativa de Dispositivos de Pentesting

Dispositivo	Precio (€)	Dificultad	Riesgo ético
Flipper Zero	150-250	Media	Alto
Rubber Ducky	50-100	Baja	Alto
Wi-Fi Pineapple	200-300	Alta	Alto
LAN Turtle	100-150	Media	Medio
Bash Bunny	120-200	Media	Alto
ESP32 devkits	5-20	Alta	Variable

8 Casos Prácticos y Escenificaciones con Actores

- Clonación de tarjeta de hotel
- Interferencia en apertura de garajes
- Red Wi-Fi trampa en evento maker

9 Demostraciones Reales sobre el Público

- Demostración controlada de ataques con consentimiento
- Feedback inmediato del público

10 Sorteo de Premios: Hackeados Premiados

- Selección aleatoria entre participantes hackeados
- Premios relacionados con el mundo maker y la ciberseguridad

11 Cierre y Reflexión Final

- Educación y concienciación como mejores defensas
- Seguridad como parte del diseño maker
- Compromiso ético en el conocimiento adquirido

12 Recursos Adicionales y Bibliografía

- *Hacking: The Art of Exploitation*
- *The Hacker Playbook*
- Plataformas: Hack The Box, TryHackMe, Root Me
- Foros: Hackaday, r/flipperzero, DEFCON, CCC