Źródła informacji do projektu

WiFi Sniffer – przechwytywanie ruchu sieciowego

Meritshot: Opisuje, jak narzędzia do sniffingu mogą być wykorzystywane zarówno przez administratorów sieci do monitorowania, jak i przez hakerów do przechwytywania poufnych danych.

https://www.meritshot.com/sniffing-in-cyber-security/

Tripwire: Przedstawia zalety i zagrożenia związane z używaniem narzędzi do sniffingu, podkreślając ich rolę w diagnozowaniu problemów sieciowych oraz potencjalne ryzyko nadużyć.

https://www.tripwire.com/state-of-security/introduction-benefits-and-risks-packet-sniffing

CyberMatters: Omówienie działania snifferów, ich mechanizmów oraz potencjalnych zastosowań w atakach typu Man-in-the-Middle

https://cybermatters.info/cyber-security/sniffing-in-cybersecurity/

BadUSB – złośliwe urządzenia USB

ManageEngine: Wyjaśnia, czym jest atak BadUSB, jak działa oraz jak się przed nim chronić.

https://www.manageengine.com/data-security/security-threats/bad-usb.html

RedZoneTech: Opisuje, jak ataki BadUSB wykorzystują zaufanie komputerów do urządzeń USB, umożliwiając wykonanie złośliwych działań.

https://www.redzonetech.net/blog-posts/bad-usb

Wikipedia: Szczegółowy opis ataków BadUSB, ich historii oraz przykładów wykorzystania w praktyce.

RFID/NFC – zagrożenia i ataki

TechTarget: Przedstawia sześć potencjalnych zagrożeń związanych z technologią NFC, w tym oszustwa płatnicze i podsłuchiwanie.

https://www.techtarget.com/whatis/feature/6-potential-enterprise-security-risks-with-NFC-technology

NCBI: Analiza zagrożeń cybernetycznych związanych z transakcjami NFC oraz strategie ich minimalizacji, ze szczególnym uwzględnieniem urządzeń płatniczych.

https://pmc.ncbi.nlm.nih.gov/articles/PMC11644477/

Wired: Opisuje, jak badacze odkryli sposób na otwieranie zamków hotelowych wykorzystujących technologię RFID, co pokazuje praktyczne zagrożenia związane z tą technologią.

https://www.wired.com/story/saflok-hotel-lock-unsaflok-hack-technique

Urządzenia haktywistyczne / narzędzia ofensywnego bezpieczeństwa (offensive security tools)

Flipper Zero, HackRF One + PortaPack H2, Proxmark3 itp.

Potencjalne zagrożenia związane z Flipper Zero i podobnymi mu urządzeniami.

https://www.normcyber.com/blog/flipper-zero-a-threat-to-your-business-or-a-novelty-gimmick/

Złośliwe ładowarki (Juice Jacking)

Atak polegający na podłączeniu urządzenia do publicznego portu USB (np. na lotnisku), przez który atakujący może zainfekować telefon lub wykraść dane.

https://www.malwarebytes.com/blog/news/2019/11/explained-juice-jacking

Keyloggery sprzętowe

Urządzenia fizycznie podłączane między klawiaturą a komputerem, które rejestrują wszystko, co użytkownik pisze – często używane w miejscach publicznych lub firmach.

https://www.scip.ch/en/?labs.20230706