ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

Katedra biomedicínské informatiky

Demonstrační platforma pro výuku kyberbezpečnosti – diskrétní lokální a vzdálené testování WiFi sítí

Demonstration platform for teaching cybersecurity – discreet local and remote testing of WiFi networks

Bakalářská práce

Studijní program:	Informatika a kybernetika ve zdravotnictví
Studijní obor:	Informační a komunikační technologie

Autor bakalářské práce:	Nicolae Ceabin
Vedoucí bakalářské práce:	doc. Ing. Karel Hána, Ph.D.

Kladno 2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Ceabin**	Jméno:	**Nicolae**	Osobní číslo:	**503359**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra informačních a komunikačních technologií v lékařství**				
Studijní program:	**Informatika a kybernetika ve zdravotnictví**				

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Demonstrační platforma pro výuku kyberbezpečnosti – diskrétní lokální a vzdálené testování WiFi sítí

Název bakalářské práce anglicky:

Demonstration platform for teaching cybersecurity - discreet local and remote testing of WiFi networks

Pokyny pro vypracování:

Proveďte rešerši problematiky ochrany bezdrátových WiFi sítí s důrazem na možnost penetrace běžně nenápadnými HW prostředky a dále s důrazem na možnost penetrace na větší vzdálenost. Na základě rešerše a vlastního studia dané problematiky navrhněte, realizujte a ověřte HW a SW systém či systémy diskrétního lokálního a vzdáleného testování bezpečnosti bezdrátových Wi-Fi sítí. Ověření (otestování) funkce systému proveďte výhradně v neveřejném pro testy vyhrazeném prostoru. Vytvořte technickou dokumentaci řešení a podrobný návod na sestavení a využití systému (systémů) při výuce.

Seznam doporučené literatury:

[1] Jirásek, P., Novák, L., Požár, J., Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. , ed. 3., Policejní akademie ČR v Praze, 2015, ISBN ISBN 978-80-7251-436-6
[2] Burda, K., Kryptografie okolo nás, ed. 1., CZ.NIC, z. s. p. o., 2019, ISBN 978-80-88168-52-2
[3] Kolouch, J., Bašta, P. a kol, CyberSecurity, ed. 1., CZ.NIC, z. s. p. o., 2019, ISBN 978-80-88168-34-8
[4] Buchanan, C., Ramachandran, V., Kali Linux Wireless Penetration Testing Beginner's Guide, ed. 3., Packt, 2017, ISBN 978-1788831925

Jméno a příjmení vedoucí(ho) bakalářské práce:

doc. Ing. Karel Hána, Ph.D.

Jméno a příjmení konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **14.02.2023**
Platnost zadání bakalářské práce: **20.09.2024**

doc. Ing. Karel Hána Ph.D.
vedoucí katedry

prof. MUDr. Jozef Rosina, Ph.D., MBA
děkan

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci s názvem „Demonstrační platforma pro výuku kyberbezpečnosti – diskrétní lokální a vzdálené testování WiFi sítí“ vypracoval samostatně a použil k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k diplomové práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně 18.5.2020 …..……..……...

Nicolae Ceabin

PODĚKOVÁNÍ

Rád bych poděkoval svému vedoucímu práce panu doc. Ing. Karlu Hánovi, Ph.D. za průběžné konzultace, dostupnost, inspiraci a cenné rady. Zároveň bych chtěl poděkovat rodině a přátelům za podporu při psaní bakalářské práce.

ABSTRAKT

Demonstrační platforma pro výuku kyberbezpečnosti – diskrétní lokální a vzdálené testování WiFi sítí

Práce se zabývá problematikou ochrany bezdrátových Wi-Fi, a to s využitím běžně nenápadných prostředků. Cílem práce bylo stavit systém na základě vlastního průzkumu, který dokáže provádět penetrační testování na větší vzdálenost pomocí bezpilotního systému. Na základě zprovoznění zařízení a otestovaní byla sestavena technická dokumentace zařízení. Při sestavení dokumentace byl kladen hlavně důraz na podrobný, ale zároveň jednoduchý postup. Tento postup bude následně využit studenty v rámci výuky, během níž se zamyslí o zabezpečení bezdrátové sítě a vyzkouší si jednotlivé zařízení. Studenti si podle technické dokumentace a návodu vyzkouší v rámci úloh instalaci operačního systému, zprovoznění zařízení a penetrační testování s využitím bezpilotního systému ve vnitřním prostoru.

Klíčová slova

Zabezpečení Wi-Fi sítě, penetrační testování, bezpilotní zařízení, kybernetická bezpečnost, výuka IT

ABSTRACT

Demonstration platform for teaching cybersecurity – discreet local and remote testing of WiFi networks

This thesis addresses the issue of protecting Wi-Fi wireless devices using normally unobtrusive means. The aim of the work was to build a system, based on a custom survey, that could perform penetration tests at a greater distance using an unmanned aircraft system. Based on the commissioning and testing of the device, technical documentation of the device was produced. The main focus of the documentation was to provide a detailed yet simple procedure. This procedure will then be used by the students in a tutorial where they will reflect on the security of the wireless network and test the different devices. The students will use the technical documentation and instructions to try out the tasks of installing the operating system, commissioning the device and penetration testing using the unmanned aircraft system indoors.

Keywords

Wi-Fi network security, penetration testing, unmanned aircraft system, cyber security, IT education

Obsah

Seznam zkratek a obrázků

Seznam zkratek

Zkratka	Význam
AP	Přístupový body (Access point)
HW	Hardware
LAN	Lokální síť (Local Area Network)
LED	Světelná dioda (Light-Emitting Diode)
MTOM	Maximální vzletová hmotnost (Maximum Take-Off Mass)
SSID	Identifikátor bezdrátové sítě (Service Set Identifier)
SW	Software
WLAN	Bezdrátová lokální síť (Wireless Local Area Network)
Wi-Fi	Bezdrátová technologie (*Wireless Fidelity)*
ÚCL	*Úřad civilního letectví*

1 Úvod

Wi-Fi sítě jsou v dnešní době nezbytnou součástí lidského života. Uživatelé mají téměř vždy při sobě zařízení pro příjem Wi-Fi signálu a snadno se připojují k bezdrátovým sítím v domácnostech, firmách a veřejných prostorech. Na světě existují různé druhy Wi-Fi přístupových bodů s různou úrovní zabezpečení. Právě tento fenomén má za důsledek vysokou zranitelnost. Mnoho uživatelů si ani neuvědomuje jednoduchost narušení jejich bezpečnosti a soukromí. V dnešní době dokáže potenciální útočník prolomit cílovou síť i bez znalostí v oblasti bezpečnosti, a to například pomocí nenápadných prostředků. S ohledem na výše uvedená rizika je důležité na problematiku zabezpečení Wi-Fi sítě co nejlépe poukázat pomocí demonstrace a vyzkoušení si sítě sami.

1.1 Cíle práce

Prvním cílem práce je analyzovat téma problematiky ochrany bezdrátových Wi-Fi sítí a seznámit čtenáře s pojmem penetračního testování. Dále prozkoumat trh s penetračními zařízeními a vybrat vhodné zařízení pro vzdálenou penetraci sítě. Navrhnout nástroj pro transport penetračního zařízení k vzdálenému bodu. Sestavit podrobnou rešerši a návrh systému z výše uvedených položek.

Vytvořit technickou dokumentaci každého vybraného zařízení. Poté sestavit podrobný návod k sestavení a použití vybraných zařízeních, který budou sloužit jako úlohy pro studenty. Návod by měl být napsán primárně srozumitelným jazykem pro laiky, aby i student bez technických znalostí o testování sítě dokázal postupovat krok po kroku.

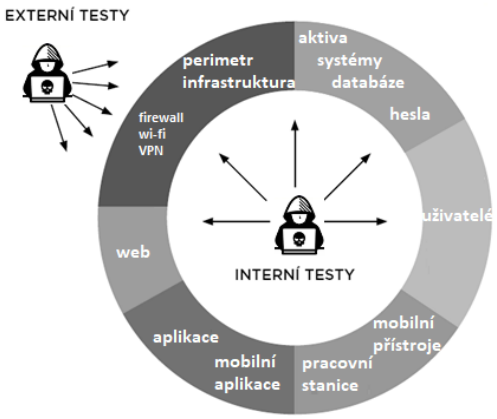
Sestavit a ověřit funkčnost systému pro penetrační testování. Vybrat neveřejný testovací prostor v souladu se zákony. Následně sepsat postup průběhu testování.

2 Přehled současného stavu

2.1 Penetrační testování

Penetrační testování je proces identifikace zranitelnosti a spočívá v simulaci útoku. Tento útok může být proveden na síť, server, počítač, aplikaci, či dokonce na osoby. Penetračním testováním se zabývá etický hacker (Ethical Hacker), který se především snaží hledat zranitelnosti v sytému, kontrolovat zabezpečení a následně provádět optimalizaci zabezpečení. Jedná se o zaškoleného a kvalifikovaného experta, který využívá strategii myšlenkové simulace útočníka a usiluje tím o dosáhnutí efektivnějšího zabezpečení systému. (1)

Existují určité faktory, které ovlivňují penetrační testování, a to znalost v oblasti testování a umístění samotného testera. Umístění se rozděluje podle toho, jestli tester provádí testování interně (například v rámci organizace) nebo externě (útok z třetí strany). Níže je uveden demonstrační obrázek (Obrázek *2.1*) typu testování podle umístění testera. Úroveň znalostí je určena tím, kolik informací a přístupů má tester k cílovému testovacímu systému. (1)



Obrázek 2.1 Ukázka interních a externích testování *(2)*

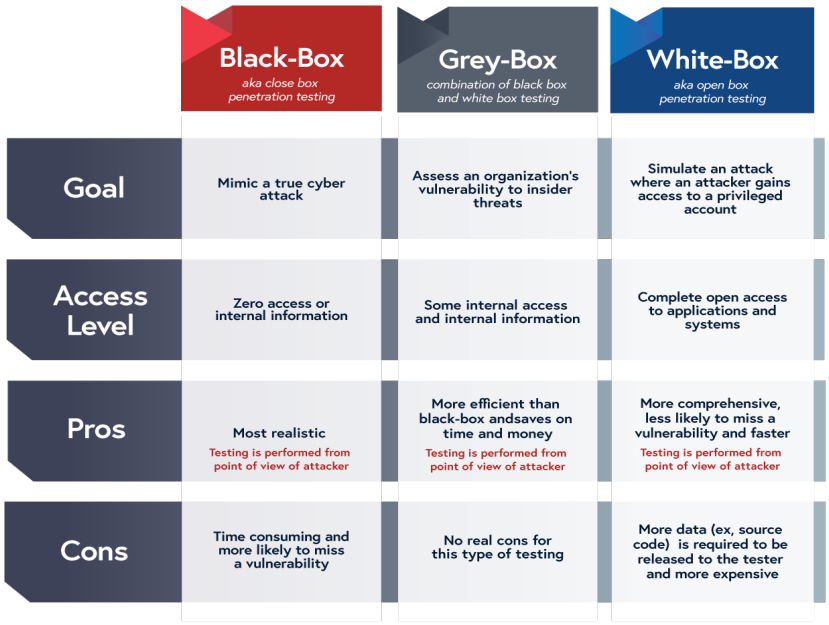
2.1.1 Umístění penetračního testování

Externí penetrační testy – cílem je simulovat útok z vnější strany a odhalit zranitelnosti, které by mohly vést k získaní neoprávněného přístupu či výpadku služeb. Jedná se především o zranitelnosti síťových služeb jako například web server, e-mail, web aplikace. (2)

Interní penetrační testy – zde je hlavním cílem zjistit zranitelnosti zevnitř. Jedná se o testy s fyzickým přístupem k sítím a testuje se situace, kdy útočník získal neoprávněný přístup do sítě. Jedná se především o testování SW služeb, operačního systému, databáze, serveru. (2)

2.1.2 Znalost prostředí

Dalším typem, na který se penetrační testování dělí, je znalost prostředí. Tato znalost se rozděluje do třech podkategorií podle úrovně znalostí, od minimální znalosti po téměř úplnou: Black-box test, White-box a Gray-box (crystal-box) (1). Níže je uveden přehledný obrázek (Obrázek *2.2*) s tabulkou rozdílů jednotlivých typů znalostí.



Obrázek 2.2 Přehled znalostí prostředí *(3)*

Black-box testování – Penetrační tester nemá téměř žádné znalosti o testovacím objektu. Pokud by se provádělo externí testování, tak tester obdrží například pouze název webové stránky nebo IP adresu a pokusí se jí prolomit. Black-box testování se používá pro ověření funkčnosti systému a zjištění kritických zranitelností (1).

White-box testování – Tester má kompletní znalost o testovacím objektu. Před testováním může tester obdržet například schéma konkrétní sítě, přístup s vysokými právy a má právo nahlížet do zdrojového kódu. Pomocí těchto znalostí je tester schopen otestovat jednotlivé části systému a ověřit jeho logické zranitelnost, bezpečnostní rizika či chybné konfigurace. Tento typ testování je komplexnější, jelikož se jedná o kombinaci interní a externí zranitelnosti. (3)

Gray-box testování – Gray-box testovaní je kombinací Black a White box testování. Tester může obdržet základní přístup do systému či jen části zdrojového kódu. Tento test simuluje útočníka, který získal přístup do interního systému prostřednictvím sítě a má k němu omezený přístup. (3)

2.2 Architektura a standardy Wi-Fi sítí

Technicky se též označuje WLAN (Wireless Local Area Network), tento název se využívá pro jakoukoli bezdrátovou sít a je ekvivalentní zkratce LAN (4). Data jsou přenášena prostřednictvím elektromagnetických radiových vln o frekvencích 2,4 GHz, 5 GHz a výjimečně 6 GHz podle standardu IEEE 802.11 (5).

2.2.1 Standardy IEEE 802.11

Standardy pro Wi-Fi (Wireless Fidelity) byly vyvinuty v roce 1997 organizací IEEE (Institute of Electrical and Electronics Engineers) a definují parametry bezdrátové sítě jako jsou rychlost přenosu dat, frekvenční pásmo, zabezpečení sítě a kompatibilitu. Existuje několik standardů IEEE 802.11 a každý z nich se liší svými parametry a použitím. V tabulce (*Tabulka 1*) je jednoduché porovnání nejznámějších standardů IEEE 802.11. (6)

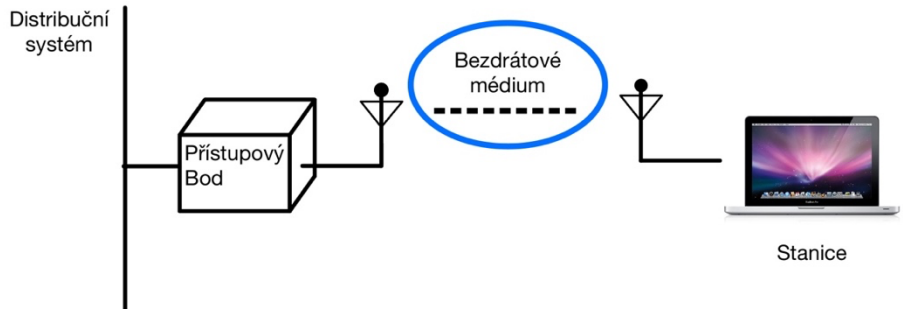
Tabulka 1 Porovnání standardů IEEE 802.11 *(7)*

Název	Frekvenční pásmo	Rychlost přenosu
802.11a	5 GHz	Až 54 Mbps
802.11b	2.4 GHz	Až 11 Mbps
802.11g	2.4 GHz	Až 54 Mbps
802.11n	2.4 GHz a 5 GHz	Až 600 Mbps
802.11ac	5 GHz	Až 1800 Mbps

2.2.2 Architektura WLAN sítí

Všechny sítě standardu 802.11 obsahují čtyři hlavní druhy fyzických komponent viz obrázek (*Obrázek 2.3*), a to distribuční systém, AP (Access point), bezdrátové médium a stanici. Distribuční systém slouží především ke komunikaci mezi jednotlivými přístupovými body a k předání informací o pohybu mobilních stanic mezi nimi. Nejčastěji je distribuční systém řešen jako kombinace sítového mostu (bridge) a distribučního média

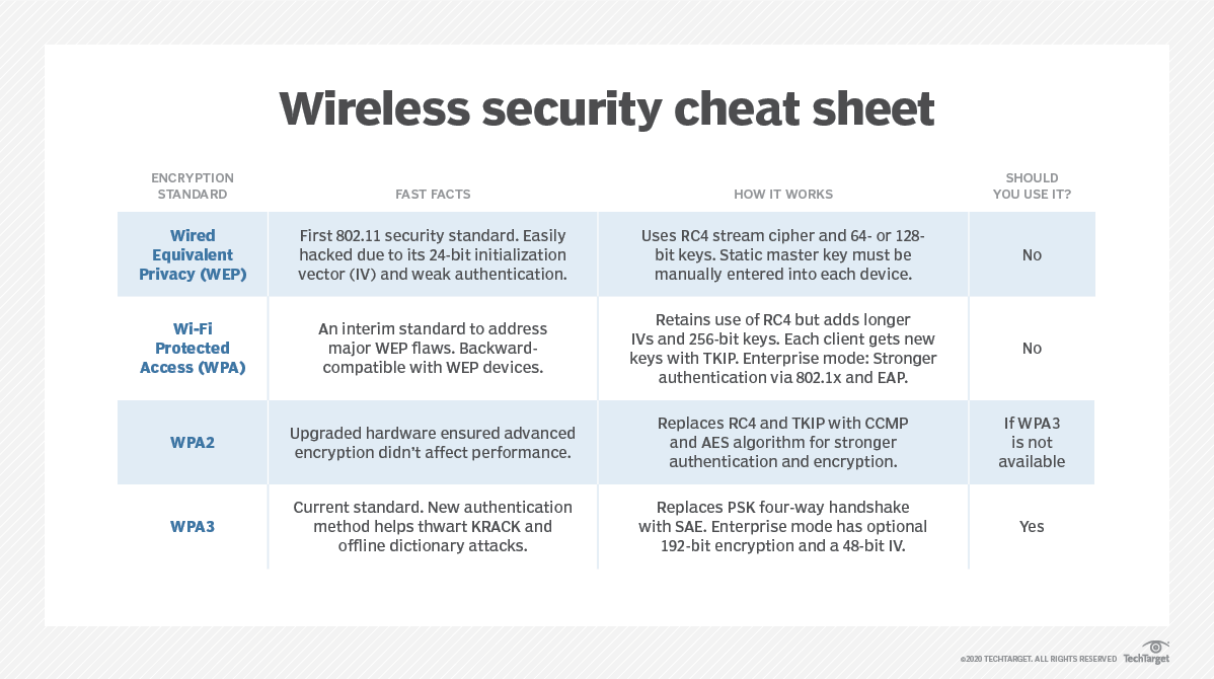
(Ethernet). Přístupový bod (AP) pak slouží k bezdrátovému připojení stanic k síti, jedná se o tzv. most mezi bezdrátovou a kabelovou částí sítě. Stanici může představovat libovolné zařízení připojené k bezdrátové sítí jako například mobilní telefon, počítač, notebook. Bezdrátové médium přenáší data ze stanice do stanice, jednoduše řečeno, plní stejnou funkci jako kabeláž pro sítě kabelové. (4)



Obrázek 2.3 Komponenty sítě WLAN. Zdroj: Autor předělal obrázek *(4)*

2.3 Ochrana bezdrátových Wi-Fi sítí

S postupným rozvojem technologie Wi-Fi a rostoucím počtem uživatelů se začaly objevovat i první bezpečnostní problémy. Z počátku technologie ochrany byla poměrně slabá a docházelo k lehké ztrátě citlivých informací, díky tomu byla též i jednoduchým terčem pro útočníky. Organizace IEEE proto začala vyvíjet různé bezpečnostní protokoly, které se postupně vyvíjeli s rozvojem Wi-Fi. Níže je uveden obrázek (Obrázek *2.4*) s krátkým popisem, každého protokolu a zda je bezpečný v dnešní době.



Wireless security cheat sheet

ENCRYPTION STANDARD	FAST FACTS	HOW IT WORKS	SHOULD YOU USE IT?
Wired Equivalent Privacy (WEP)	First 802.11 security standard. Easily hacked due to its 24-bit initialization vector (IV) and weak authentication.	Uses RC4 stream cipher and 64- or 128-bit keys. Static master key must be manually entered into each device.	No
Wi-Fi Protected Access (WPA)	An interim standard to address major WEP flaws. Backward-compatible with WEP devices.	Retains use of RC4 but adds longer IVs and 256-bit keys. Each client gets new keys with TKIP. Enterprise mode: Stronger authentication via 802.1x and EAP.	No
WPA2	Upgraded hardware ensured advanced encryption didn't affect performance.	Replaces RC4 and TKIP with CCMP and AES algorithm for stronger authentication and encryption.	If WPA3 is not available
WPA3	Current standard. New authentication method helps thwart KRACK and offline dictionary attacks.	Replaces PSK four-way handshake with SAE. Enterprise mode has optional 192-bit encryption and a 48-bit IV.	Yes

Obrázek 2.4 Jednoduchý přehled jednotlivých protokolů. Zdroj: *(8)*

2.3.1 WEP

Protokol WEP (Wired Equivalent Privacy – Bezpečnost jako drát) byl založen v roce 1997 a stal se součástí standardu IEEE802.11. Cílem bylo zabezpečit komunikaci mezi přístupovým bodem a stanicí, aby odpovídala zabezpečení LAN. K šifrování se využívá proudový šifrovací symetrický bitový klíč RC4 (Rivest Cipher 4). Tento klíč zůstává po celou dobu stejný a ukládá se přímo do zařízení a díky tomu může dojít k jednoduchému odcizení klíče. Vzhledem k tomu, že klíč zůstává po celou dobu statický, lze ho snadno prolomit hrubou silou (BruteForce). Existuje jen určité množství kombinací, a proto pro dnešní počítače to nedělá žádný problém najít správnou kombinaci klíče. Mezi další nevýhody tohoto protokolu patří to, že využívá identický klíč pro šifrování a dešifrování. V roce 2001 byl protokol WEP zcela prolomen a dnes se již považuje za zastaralý. (9) (10) (11)

2.3.2 WPA

Protokol WPA (Wi-Fi Protected Access – Chráněný přístup Wi-Fi) byl vydán jako přímá reakce na nedostatky a zranitelnost svého předchůdce WEP. WPA využívá stejný algoritmus předchůdce pod názvem RC4, avšak je doplněn o technologii TKIP (Temporal Key Integrity protokol), který pravidelně mění šifrovací klíč každých 10 000 paketů (balíček informací). Právě tímto je zmírněno riziko prolomení šifrovacího klíče, jelikož nový klíč bude vygenerován dříve, než útočník ho stihne prolomit. Hlavní výhodou WPA je jeho zpětná kompatibilita s WEP. WPA protokol se již nevyužívá hlavně kvůli algoritmu RC4, který je dnes už snadno prolomitelný. (11) (12)

2.3.3 WPA2 a WPA3

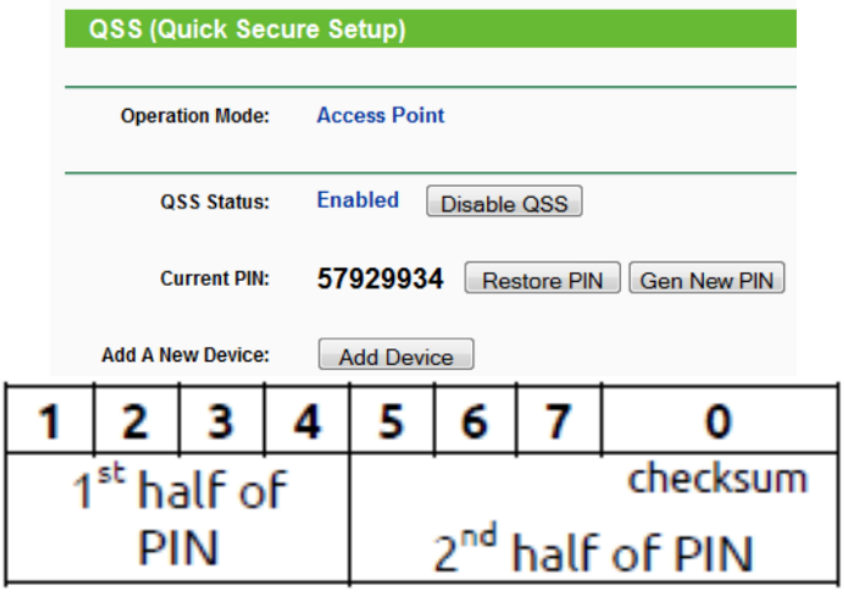
WPA byl později nahrazen novým protokolem WPA2, který přidává zásadní vylepšení šifrování pomocí algoritmu CMMP realizovaný na AES (Advanced Encryption Standard). Jedná se o blokovou šifru, ve které je každá zpráva rozdělena a určité bloky o stejné délce. Každý blok je zašifrován nezávislé na ostatních. Protokol WPA2 je zpětně kompatibilní s WPA, a proto stále zahrnuje TKIP. Přesto tento protokol není zcela bezpečný. (10) (12)

V roce 2017 byly zveřejněny informace o chybě v protokolu Národním úřadem pro kybernetickou a informační bezpečnost. Jednalo se o chybu při přihlašování klientské stanice k přístupovému bodu. Této komunikaci se říká 4-way handshake, jelikož dojde k výměně čtyř paketů za účelem ověření pravosti hesla k bezdrátové síti a sestavení šifrovacích klíčů pro další komunikaci.
„*Útočník donutí oběť přeinstalovat již používané klíče. Při sestavovací komunikaci (4-way handshake) dochází k zápisu šifrovacího klíče po přijmu zprávy č.3. Tato zpráva však nemusí být správně doručena, proto má protistrana možnost zprávu odeslat opakovaně. Opakovaným posláním a správným doručením však dojde k přepisování klíče a zároveň resetu hodnot jako „transmit packet number (nonce)“ a „receive packet number (replay counter)“. Útočník tak může tyto hodnoty ovlivnit a využít jejich znalosti k rozklíčování komunikace*.“ (13)

V posledních letech se aktivně začal rozvíjet protokol WPA3, který opravuje zranitelnosti předchůdce.

2.3.4 WPS

Zabezpečení WPS (Wi-Fi Protected Setup) umožňuje jednoduché připojení k bezdrátové síti prostřednictvím dekadického PIN kódu nebo tlačítka WPS, který se nachází na routeru. Zařízení, které se chce připojit posílá osmimístný PIN do routeru a poté čeká na odpověď. PIN se skládá ze tří částí a celkem tvoří osmimístní číslo, což odpovídá 100 milionů možných kombinací. První část je tvořena prvním čtyřčíslím, druhá část odpovídá pozici 5 až 7 kódu a třetí část je poslední pozice kódu pod názvem kontrolní součet viz obrázek (*Obrázek 2.5*). Jedná se o součet všech pozic od 1 do 7. Při obdržení špatného PIN kódu router odešle zpět informaci o tom, že tento PIN je nesprávný. Zároveň se zprávou se odešle i informace, zda některá z částí PIN kódu byla správná. Tím se sníží možný počet kombinací na 11000. Právě tato bezpečnostní slabina WPS umožňuje útočníkům prolomit kód pomocí hrubé síly. (14) (15)



Obrázek 2.5 Struktura PIN kódu WPS. Zdroj: *(14)*

2.4 Zařízení pro penetrační testování

Zařízení pro penetrační testování je hardwarové zařízení či software určené k detekci zranitelností v systémech a sítí. Může se jednat o zařízení přímo určené k testování či speciální programy/aplikace, které provádí testování pomocí hardwarů například telefonu, počítače, hodinek. Tester si volí potřebný nástroj podle konkrétního typu testování. Proto je důležité při výběru zařízení pro vzdálenou penetraci Wi-Fi sítí zohlednit několik faktorů jako jsou velikost zařízení, hmotnost, jednoduchost používání a samostatnost v používaní. Na trhu existuje velké množství penetračních zařízení pro testování Wi-Fi sítí, avšak obvykle se jedná o periferní zařízení. Nutné je proto vybrat zařízení, které dokáže pracovat samostatně bez nutnosti drátového připojení k počítači. (16)

Po prozkoumání trhu byly zvolena dvě zařízení, které by odpovídala požadavkům pro vzdálené penetrační testování. Prvním zařízením je Deather Watch, zařízení speciálně navržené pro penetrační testování Wi-Fi sítí. Druhým zařízením jsou chytré hodinky Mobvoi TicWatch. Tyto chytré hodinky jsou prvním produktem na světě, který podporuje instalaci operačního systému NetHunter. Jedná se o mobilní operační systém postavený na volně distribuovaném Linuxu, který slouží výhradně k testování. (17) (18)

2.4.1 Deauther Watch Wi-Fi Hacking V2

Deauther Watch je malé zařízení od společnosti DSTIKE, které vypadá jako chytré hodinky viz obrázek (Obrázek *2.6*) a primárně slouží k testování okolních Wi-Fi sítí. Toto zařízení je uživatelsky přívětivé, a to díky jeho velikosti, výdrži baterie a programovatelnosti podle vlastních potřeb.

Obrázek 2.6 Deauther Watch V2. Zdroj: *(19)*

Zařízení využívá vývojovou desku ESP8266, což je malý a výkonný mikrokontrolér, který umožňuje vysokou programovatelnost a flexibilitu zařízení. S baterií o kapacitě 800mAH poskytuje Deauther Watch V2 poměrně dlouhou výdrž a to až 8 hodin, což je pozoruhodné vzhledem k jeho malým rozměrům a vysokému výkonu. (20)

Mezi hlavní funkce testovacího zařízení patří například možnost odpojit uživatele od Wi-Fi sítě, vytvořit falešnou Wi-Fi síť (tzv. fake AP) a zobrazit provoz na Wi-Fi síti. Je důležité zdůraznit, že tyto funkce jsou určeny pouze pro účely testování bezdrátových sítí a neoprávněné použití může být v rozporu se zákony. Níže je uvedena tabulka (Tabulka *2*) se všemi technickými specifikacemi pro verzi V2, poskytnutými výrobcem z webové stránky DSTIKE (17).

Tabulka 2: Specifikace zařízení Deauther Watch *(17)*

	Deauther Watch V2
Displej	1.3" OLED
Baterie	800 mah
Napájení	0.8 A
Výdrž baterie	7-8 h
Hmotnost	61 g
Velikost (DxŠxV, mm)	55x50x19

2.4.2 Chytré hodinky TicWatch Pro 3

TicWatch Pro 3 jsou chytré hodinky od společnosti Mobvoi viz obrázek (Obrázek *2.7*), běžící na operačním systému WearOS, který vyvinut společností Google. Zařízení je kompatibilní se smartphony od společností Apple a Google a podporuje všechny základní funkce moderních chytrých hodinek. (21)

Obrázek 2.7 Hodinky TicWatch Pro 3. Zdroj: *(22)*

Mezi hlavní výhody hodinek je velký dotykový displej s úhlopříčkou 1,4 palce, voděodolnosti dle standardu IP68 a dlouhou vydrží baterie až 72 hodin. TicWatch Pro 3 jsou vybaveny senzory pro měření sportovních aktivit, monitorování srdečního tepu, tlaku a spánku. (21)

TicWatch plně podporuje instalaci operačního systému NetHunter, a proto je možné využít tyto hodinky pro účely testování bezdrátových sítí. Systém je založen na distribuci Kali Linux a slouží především k penetračnímu testování. NetHunter podporuje bezdrátové adaptéry, takže síť lze testovat pomocí HW adaptéru chytrých hodinek. NetHunter poskytuje uživatelům mnoho užitečných funkcí a nástrojů pro testování sítí a vyhledávání bezpečnostních chyb. (21)

Jednou z hlavních nevýhod nákupu TicWatch hodinek je skutečnost, že v balení nejsou k dispozici čtyřpinové USB konektory pro přenos dat, ale pouze dvoupinové pro nabíjení zařízení. Tyto čtyřpinové konektory nelze běžně zakoupit, avšak je možné si je vyrobit podle návodu. (23)

2.4.3 Operační systém NetHunter

NetHunter je operační systém určený pro mobilní zařízení na platformě Android, který vyvinula společnost Offensive Security. Společnost je známá především díky svému operačnímu systému Kali Linux, na kterém byla vyvinuta mobilní a odlehčená verze NetHunteru. NetHunter poskytuje uživatelům řadu nástrojů pro monitorování zabezpečení, včetně monitorování bezdrátových sítí a skenování útoků a zranitelností. NetHunter lze nainstalovat do většiny zařízení se systémem Android, takže uživatelé mají k dispozici mobilní zařízení pro penetrační testování. Kromě instalace do mobilních zařízení lze NetHunter nainstalovat také do chytrých hodinek. Hodinky TicWatch Pro 3 Ultra běžící na operačním systému WearOS oficiálně podporují instalaci programu NetHunter. To znamená, že uživatelé těchto hodinek mohou pomocí vestavěného bezdrátového adaptéru zkontrolovat svou síť a najít bezpečnostní zranitelnosti. Díky této

mobilitě je NetHunter velmi oblíbeným nástrojem v oblasti kybernetické bezpečnosti a etického hackingu. (24)

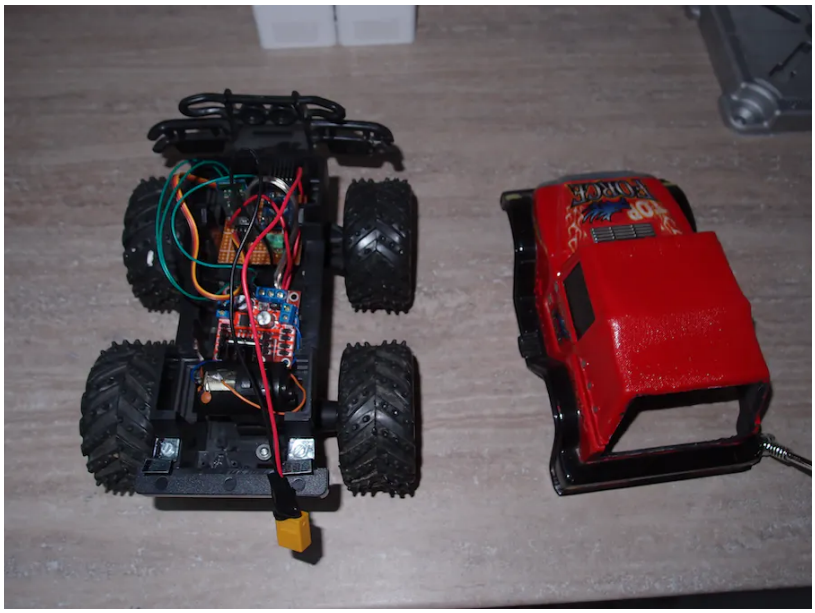
2.5 Penetrace na větší vzdálenost

Při návrhu systému pro penetraci sítě na větší vzdálenost je důležité zvážit několik faktorů: vzdálenost a dostupnost testovacího objektu, poměrně malé rozměry přenosného zařízení a výdrž v závislosti na výkonu zařízení. Zařízení pro přepravu testovacího HW by mělo být rovněž nenápadné, aby bylo nejlépe nasimulováno napadení na objekt. Mezi zařízení, která by splňovala požadavky pro systém penetrace sítě, by mohla patřit například tato: autíčka na dálkové ovládání, drony či malý robotický pes.

2.5.1 Porovnání zařízení pro vzdálené penetrační testování

2.5.1.1 Mobilní zařízení na dálkové ovládání (autíčko)

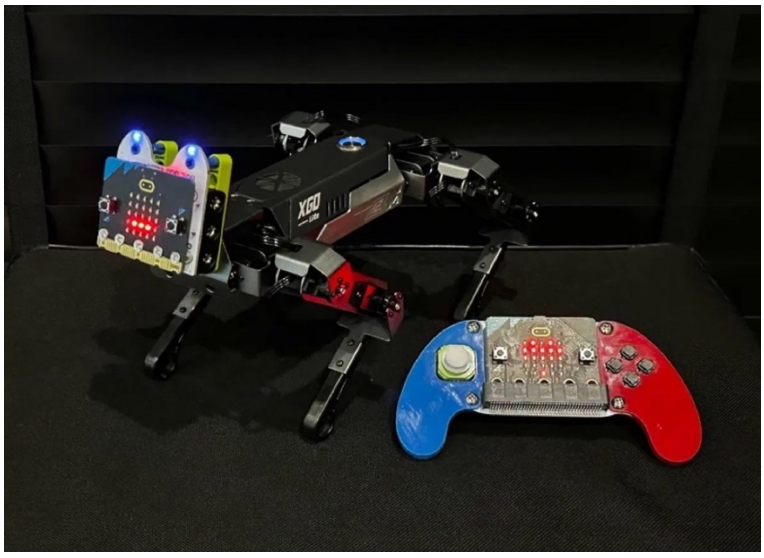
Mezi hlavní výhody autíčka s dálkovým ovládáním jsou jeho poměrně malé rozměry, výdrž baterie a velká dostupnost. V závislosti na rozměrech autíčka je taktéž možné úkryt testovací HW pod jeho konstrukci stejně jak na obrázku (*Obrázek 2.8*). Mezi nedostatky autíčka s dálkovým ovládáním patří jeho lehké ztracení mezi objekty, které by bylo možné vyřešit upevněním 360° kamery s bezdrátovým vysíláním obrazu do telefonu. Další nevýhody jsou jeho vysoká viditelnost v terénu pro cílový subjekt a v závislosti na terénu jeho lehké zaseknutí.



Obrázek 2.8 Auto na dálkové ovládání. Zdroj: *(25)*

2.5.1.2 Robotický pes

Robotický pes je typ robota, který je navržen k provádění určitých úkolů na těžko přístupných místech. Robot je vybaven pohyblivými nohami a senzory pro vnímání okolí a díky tomu je schopen manévrovat v různém terénu. V dnešní době je robotický pes využíván především při vojenských operacích nebo záchranných akcích. Na trhu se ale začal prodávat i robotický pes pro veřejnost viz obrázek (*Obrázek 2.9*), který svým chováním připomíná domácího mazlíčka a může být ovládán na dálkové ovládání.

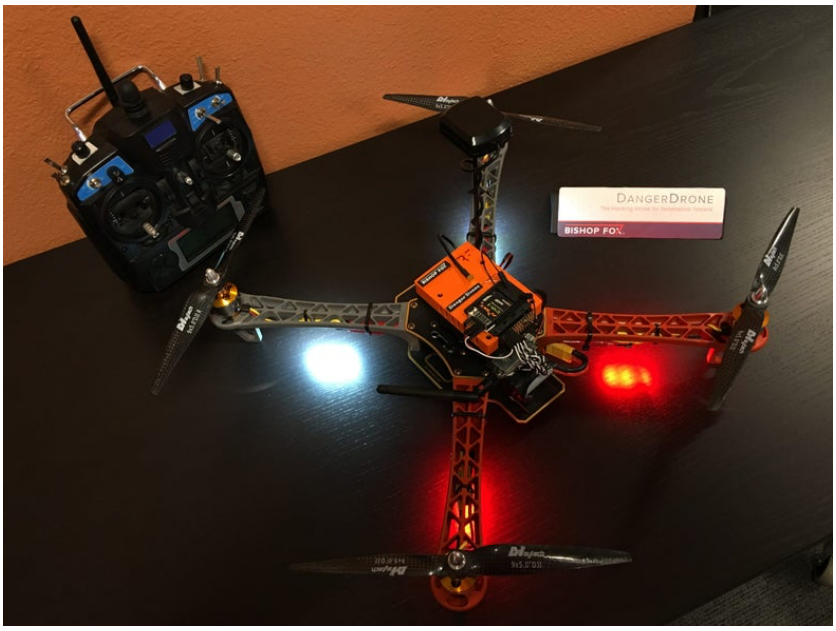


Obrázek 2.9 Robotický pes XGO Robot. Zdroj: *(26)*

Robotický pes oproti autíčku na dálkové ovládání umí lépe manévrovat mezi objekty, je snadno maskovatelný v terénu a taktéž méně hlučný. Vzhledem k jeho konstrukci se dokáže snadněji pohybovat na náročném terénu jako jsou schody, nerovnosti, či různé překážky. Nevýhodou robotického psa je vzhledem k jeho slabším prodejům jeho dostupnost. Má rovněž identickou nevýhodu jako autíčko na dálkové ovládání, a to lehké ztracení mezi objekty, které by bylo nutné vyřešit kamerou.

2.5.1.3 Bezpilotní systém – Dron

Drony neboli bezpilotní letecké prostředky jsou dnes již běžně využívány pro různé účely jako například monitorování, průzkum či pořizování videozáznamu. V závislosti na využití jsou drony vybaveny různými senzory, jako jsou kamery, GPS moduly, termokamery nebo dokonce i senzory pro monitorování znečištění ovzduší. Mohou být ovládány pomocí dálkového ovladače nebo autonomním softwarovým systémem. Využití dronů pro vzdálené penetrační testování má několik výhod, jako například: Přístup do míst, která jsou pro člověka těžko dostupná. Stejně tak velký dolet dronu, jeho rychlost a dostupnost. Přestože drony by mohli být ideální volbou pro vzdálené penetrační testovaní sítě je taktéž nutné zohlednit i některé nedostatky, mezi které patří: Pravidla nařízení, které mohou omezit provoz dronů v testovacím prostoru. Nezbytné je též mít doklad o absolvování online výcviku od úřadu pro civilní letectví, a to minimálně kategorii A1 a A3. Níže je uveden příkladový obrázek (*Obrázek 2.10*) jak by mohl penetrační systém vypadat.



Obrázek 2.10 Ilustrační obrázek drona a modulu Rasberry Pi. Zdroj: *(27)*

2.5.2 Porovnání bezpilotních zařízení

Na základě porovnání několika možností pro přepravu HW zařízení na testování sítě jsem se rozhodl vybrat dron, který má méně nedostatků týkající se pohybu v terénu a viditelnosti v prostoru. V současné době je na trhu rozsáhlé množství výběru bezpilotního systému a při výběru je důležité zohlednit jeho parametry v závislosti na potřebách testování: Cena, nosnost, výdrž baterie, funkce (autostart, autopřistání, online přenos).

Po provedení průzkumu trhu byla vytvořená jednoduchá tabulka (Tabulka *3*) s porovnáním nejlepších možností pro bezpilotní zařízení na základě ceny a charakteristik. Následně bylo zvoleno zařízení DJI Mini 2 SE Fly, jelikož je z hlediska požadovaných parametrů srovnatelný s konkurencí a je cenově dostupnější.

Tabulka 3: Porovnání bezpilotních zařízení. Zdroj: *(28) (29) (30)*

	DJI Mini 3 Pro	DJI Mini 2 SE	Autel EVO Nano+
Doba provozu	34 min	31 min	28 min
Dosah přenosu	12 km	10 km	10 km
Max. rychlost	57,6 km/h	57 km/h	54 km/h
Hmotnost	249 g	249 g	249 g
Rozměry (ŠxVxH)	6,2 x 9 x 14,5 cm	13,8 x 20,3 x 5,6 cm	9,4 x 5,5 x 14,2 cm
Cena	20 831 Kč	12 244 Kč	17 490 Kč

2.5.3 Dron DJI Mini SE

Dron DJI Mini 2 SE splňuje podmínky využití pro vzdálené penetrační testování. Vzhledem k jeho malým rozměrům a lehkosti je ideálním zařízením pro mobilní využití. Výhodou je taktéž 30minutová maximální doba letu s možností přímého přenosu videa na vzdálenost až 10 km (28). Tento přenos funguje přes chytrý telefon a nevyžaduje koupi drahého ovladače (28). Přímý přenos videa není podmínkou pro vzdálené penetrační testování, avšak to může zjednodušit přístup na obtížná místa. Mezi jeho další funkce patří inteligentní návrat domů, který se může hodit v případě ztráty z dohledu zařízení (28). Kombinace těchto funkcí a cenové dostupnosti činí z tohoto zařízení ideální volbu pro penetrační testování ve srovnání s jinými modely. Výhodou zařízení je taktéž plný manuál a instrukce k provozu dronu, které jsou dostupné na oficiální webové stránce výrobce.

2.5.4 Pravidla a zkouška pilota bezpilotního systému

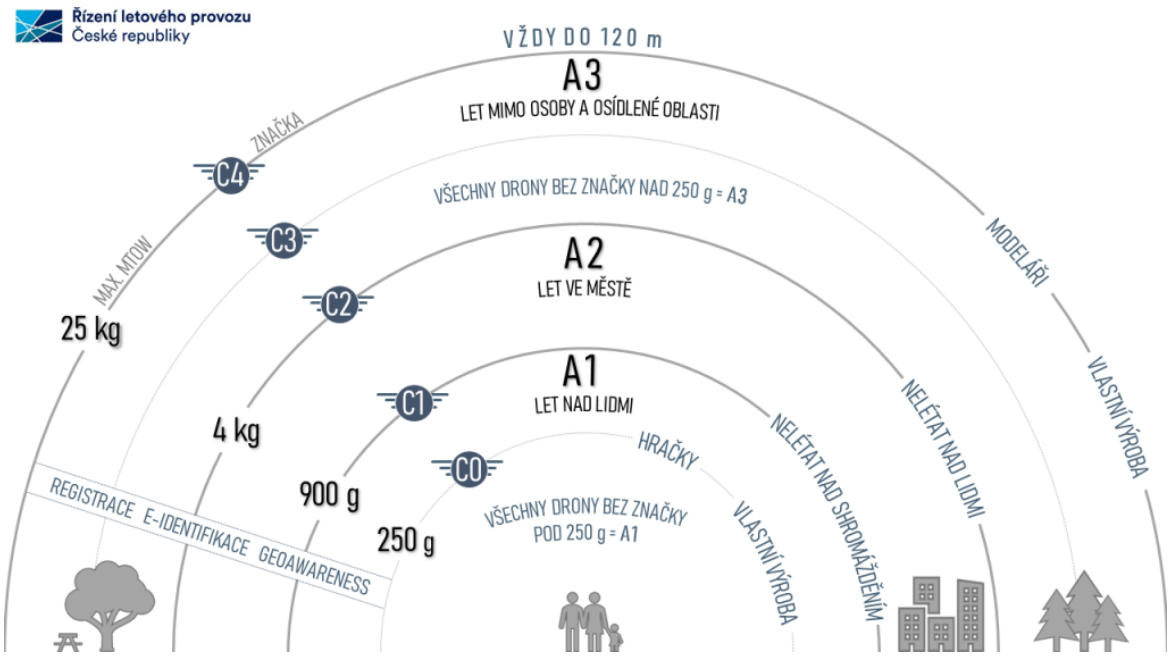
Pro uživatele bezpilotních systému je nutné se seznámit s jednotlivými pravidly EU pro létaní s drony, registrovat se jako provozovatel bezpilotních systému a případně absolvovat online zkoušku pilota. Provozovatelem dronu se považuje jakákoli osoba, která vlastní dron(y) nebo si dron pronajímá. Registrace provozovatele bezpilotního

systému je nutná v případě, že dron váží více než 250 g, nejedná se oficiálně o hračku a má na sobě kameru nebo jiný senzor schopný, jakkoliv zachycovat osobní údaje. (31)

Registrace probíhá online na webu ÚCL (Úřad pro civilní letectví) přes e-identitu. Tato registrace probíhá jen jednou a platí po celé EU. Po registraci uživatel obdrží registrační číslo provozovatele, které slouží k identifikaci provozovatele dronu (31). Následně je nutné absolvovat zkoušku pilota bezpilotního systému podle podkategorií pod názvem OPEN, a to A1 až A3. Níže je uvedená tabulka (Tabulka 4) rozdílu kategorií provozu a přehledný obrázek (Obrázek *2.11*).

Tabulka 4 Určení kategorie provozu OPEN z oficiálních stránek CAA *(32)*

Podkategorie „otevřené“ kategorie provozu	Štítek s označením třídy typu dronu
A1 Urbanistické oblasti, ale ne nad davy, nebo mimo urbanistické oblasti	Štítek s označením třídy C0, C1
	Soukromě zhotovený dron s MTOM < 250 g a rychlostí < 19m/s
	Dron bez štítku s označením třídy s MTOM < 500 g (do 31.12.2023)
	Dron bez štítku s označením třídy MTOM < 250 g včetně paliva a užitečného zatížení. (od 31.12.2023)
A2 Urbanistické oblasti při udržování nejméně 30 m (ve zvláštních případech až 5 m) od lidí, nebo mimo urbanistické oblasti.	Štítek s označením třídy C2
	Dron bez štítku s označením třídy s MTOM < 2 kg (do 31.12.2023) (Minimální vzdálenost od osob je v tomto případě navýšena na 50 m)
A3 Mimo urbanistické oblasti	Štítek s označením třídy C2
	Soukromě zhotovený dron s MTOM < 25 kg
	Dron bez štítku s označením třídy s MTOM < 25 kg



Obrázek 2.11 Určení kategorie OPEN *(32)*

Dron DJI 2 Mini SE podle oficiální tabulky od ÚCL a parametrů od výrobce spadá do kategorie OPEN, pro kterou je nutno absolvovat online zkoušku. Zkouška se skládá ze 40 otázek s výběrem správné odpovědi a časovým limitem 60 minut (33). Test se skládá z následujících témat: letecká bezpečnost, omezení vzdušného prostoru, předpisy týkající se letectví, omezení lidské výkonnosti, provozní postupy, obecné znalosti o bezpilotních systémech (33). K úspěšnému složení testu je nutno získat 75 % správných odpovědí (33). Po úspěšném absolvování testu obdrží pilot e-mailem doklad o absolvování online výcviku, který vypadá podle vzoru na obrázku (*Obrázek 2.12*). Tento doklad umožňuje létat v podkategoriích provozu A1 a A3.

Obrázek 2.12 Doklad o absolvování online výcviku. Zdroj: Autor

3 Implementace

3.1 Manuál k Deauther Watch Wi-Fi Hacking V2

Následující odstavec slouží především k popsaní fyzických prvků zařízení Deauther Watch, včetně ovládacích prvků a indikátorů stavu hodinek. Podrobnější a přehlednější popis jednotlivých prvků je uveden na obrázku, který zahrnuje i konkrétní umístění na hodinkách. Na přední straně pod displejem se nachází zapínací a vypínací tlačítko. Pro zapnutí zařízení stačí jen jednou zmáčknout tlačítko. Avšak pro vypnutí se toto tlačítko musí přibližně dvacet vteřin podržet. Hlavní stav hodinek se nachází nad displejem a je zobrazen pomocí jedné LED diody (modrá barva signalizuje skenování okolních sítí, červená útok a zelená označuje, že zařízení je v neaktivním stavu). Na pravé straně je umístěno posouvací tlačítko, které slouží primárně k ovládání menu a potvrzení akce stisknutím kolečka dovnitř. Na levé části jsou umístěny dvě tlačítka a čtyři LED diody, které zobrazují aktuální stav baterie zařízení (25 %, 50 %, 75 %, 100 %). Horní tlačítko je určeno k opětovnému skenování sítí v okolí a dolní tlačítko při delším stisknutí resetuje celé zařízení. Následující obrázek (Obrázek *3.1*) přehledně popisuje každou komponentu penetračního zařízení.

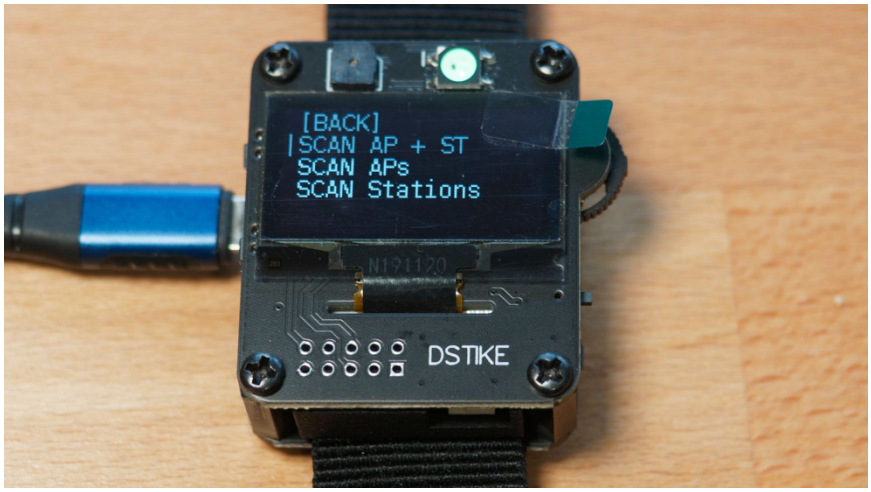
Obrázek 3.1: Schéma s popisem zařízení Deauther Watch V2. Upraveno, Zdroj: *(19)*

3.2 Návod k Deauther Watch Wi-Fi Hacking V2

Po zapnutí zařízení dojde k provedení skenování okolních přístupových bodů a následných stanic, což je signalizováno rozsvícením modré LED diody. Po dokončení skenování se zobrazí hlavní menu hodinek a rozsvítí se zelená LED dioda, indikující že zařízení je připraveno k použití. Dále jsou popsány jednotlivé funkce Deauther Watch V2.

3.2.1 SCAN

1) SCAN – Funkce SCAN slouží primárně k opakovanému skenování okolních zařízení, včetně přístupových bodů (Wi-Fi) a stanic. Toto skenování se provádí při zapnutí zařízení a poté může být opakováno pomocí funkce SCAN. Uživatel dále má na výběr tři možnosti skenování viz obrázek (Obrázek *3.2*). (34)



Obrázek 3.2: Ukázka funkce SCAN. Zdroj: *(34)*

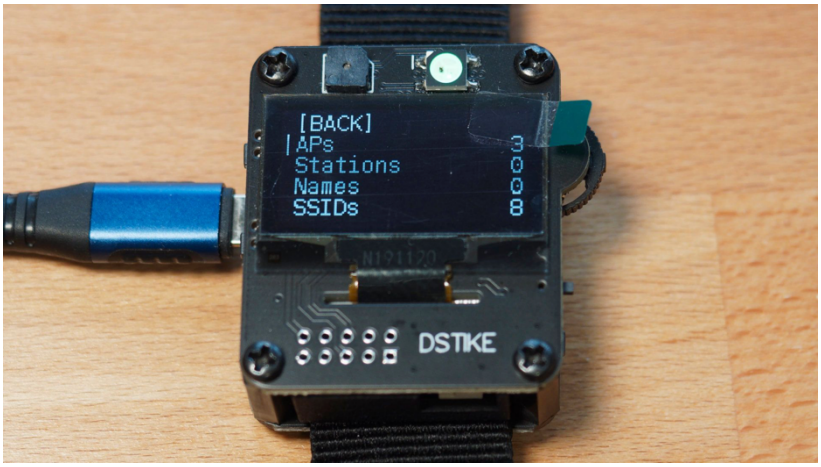
2) SCAN AP + ST – Volba provede skenování jak přístupových bodů, tak i stanic v okolí. Seznam zobrazí všechna nalezená zařízení. (34)

3) SCAN APs – Tato volba provede skenování pouze přístupových bodů v okolí. Seznam zobrazí pouze nalezené přístupové body. (34)

4) SCAN Stations – Tato volba provede skenování pouze stanic v okolí. Seznam zobrazí pouze nalezené stanice. (34)

3.2.2 SELECT

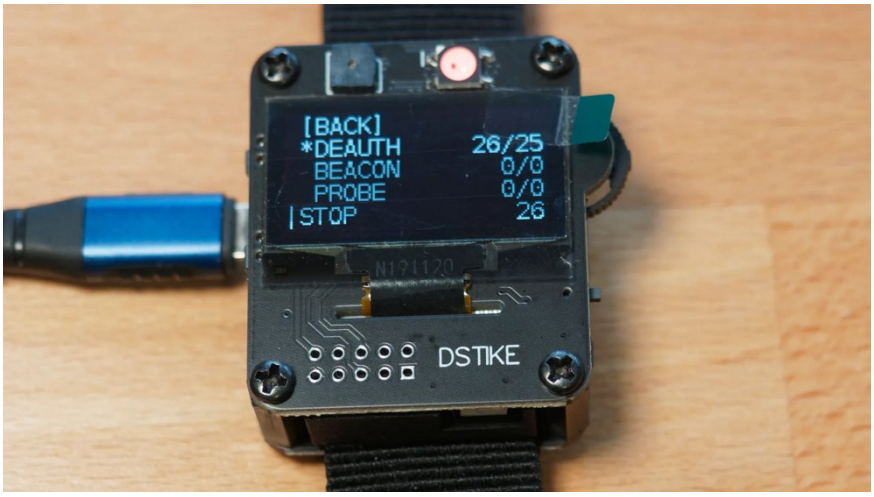
Funkce SELECT umožňuje vybrat konkrétní útok, který chceme provést. Na výběr je několik možností viz obrázek (Obrázek *3.3*), jako například ze všech naskenovaných přístupových bodů a stanic, nebo si můžeme vybrat podle jména a SSID. Tato funkce je k dispozici po provedení skenování a následně po zvolení možnosti SELECT. (34)



Obrázek 3.3: Ukázka funkce SELECT. Zdroj: *(34)*

3.2.3 Attack

V sekci attack už probíhají konkrétní testování Wi-Fi sítě. Tester má na výběr tři možné útoky: DEAUTH, BEACON, PROBE. Možnosti jsou uvedeny na obrázku (Obrázek *3.4*)



Obrázek 3.4: Ukázka funkce Attack. Zdroj: *(34)*

1. DEATH – Tento útok primárně slouží k odpojení všech připojených uživatelů od sítě. Po spuštění útoku nemají uživatelé možnost se na přístupový bod připojit, dokud není útok zastaven. (34)

2. BEACON – Po zvolení vybraného AP se provádí tzv. Beacon Flood, který generuje velké množství falešných Beacon rámců s identickým SSID jako zvolený AP. Tyto falešné Beacon rámečky mohou vést k problémům při připojení některých zařízení na správnou síť, jelikož některá zařízení mohou být “zmatená“ a pokusí se připojit k falešnému AP. (34)

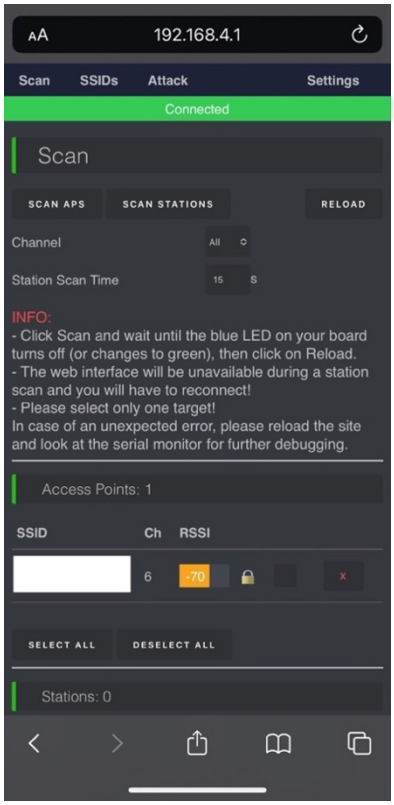
3. PROBE – Útok je podobný útoku Beacon Flood, ale místo generování falešných Beacon rámců se útočník zaměřuje na generování velkého množství "Probe Request" rámců. (34)

3.2.4 Packet Monitor

Zařízení nabízí jednoduchou možnost sledování paketů (rámců) pomocí grafu v reálném čase, počtu rámců a kanálu, na kterém se uživatel právě nachází. Mezi kanály se lze snadno přepínat pomocí kolečka (nahoru a dolů). Číslo v hranatých závorkách označuje pakety Death, což umožňuje uživateli snadno zkontrolovat, zda se v jeho okolí nevyskytují žádné aktivní útoky. (34)

3.2.5 Vzdálené ovládání

Deauther Watch umožňuje dokonce i vytvoření vlastní Wi-Fi sítě (tj. serveru) pro vzdálené ovládání a nastavování parametrů zařízení. Pro připojení k této síti je třeba se připojit k Wi-Fi síti s názvem "pwned" a zadat heslo "deauther". Poté stačí zadat do prohlížeče adresu 192.168.4.1 a stránka bude přesměrována na webové rozhraní viz obrázek (Obrázek *3.5*). Zde je možné provádět stejné funkce jako na hodinkách a také změnit název sítě nebo heslo. (34)



Obrázek 3.5 Ukázka vzdáleného přístupu přes mobilní zařízení. Zdroj: Snímek obrazovky

3.2.6 Další možnosti

Kromě základních funkcí nabízí Deauther Watch několik doplňkových možností. Patří sem například zobrazení času v 24h formátu, což umožňuje používat zařízení jako hodinky. Dále lze využít zabudovanou LED baterku.

3.3 Návod pro výrobu čtyřpinového konektoru pro TicWatch Pro 3

Pro výrobu čtyřpinového USB konektoru je nutné si pořídit nabíjecí dock s přenosem dat určený pro starší verzi TicWatch PRO a mít k dispozici 3D tiskárnu. Následně lze postupovat podle návodu:

1) Pomocí 3D tiskárny si vytiskněte kryt pro datový kabel podle modelu uvedeného na webové stránce: https://thangs.com/designer/yesimxev/3d-model/TicWatch%20Pro%203%20Micro%20USB%20Data%20Dock-59021

2) Odstaňte z nabíjecího docku gumovou část, která je znázorněná červenou šipkou na obrázku (*Obrázek 3.6*).

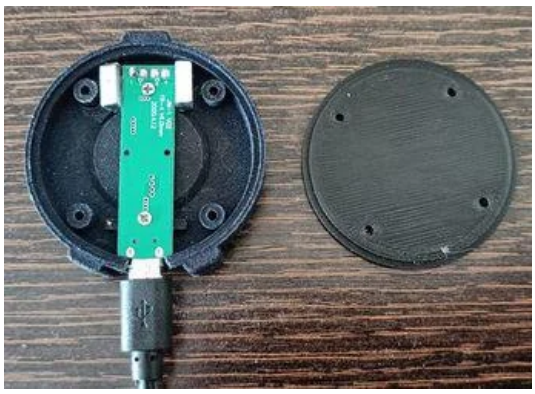
Obrázek 3.6: Gumová část nabíjecího docku. Upraveno, Zdroj: *(23)*

3) Následně odšroubujte pod gumovým krytím čtyři šroubky.

4) Poté vyjměte nabíjecí obvod a dva magnety podle obrázku (Obrázek *3.7*) z plastového docku.

Obrázek 3.7: Rozložení magnetů a nabíjecího obvodu nabíjecího docku. Upraveno, Zdroj: *(23)*

5) Vložte nabíjecí obvod a magnety do nově vytištěného krytu podle návodu na obrázku (Obrázek 3.8) a utáhněte šroubky.



Obrázek 3.8 Správné rozložení nabíjecího obvodu a magnetů v novém nabíjecím docku. Zdroj: *(23)*

3.4 Návod a příprava k instalaci operačního systému NetHunter

Autor úspěšně provedl instalaci operačního systému NetHunter na chytrých hodinkách TicWatch Pro 3 GPS pomocí vyrobeného datového kabelu a s využitím operačního systému Windows 10. Podle oficiální dokumentace od společnosti OffSec, která se zabývá distribucí Nethunteru je možné taktéž provést instalaci pomocí operačního systému Linux (18). Avšak tento návod popisuje podrobný postup instalace s využitím Windows 10.

3.4.1 Příprava instalace operačního systému NetHunter

Před samotnou instalací je nutné provést několik kroků a připravit počítač ke správné komunikaci s chytrými hodinkami. První záležitostí je nástroj Android Debug Bridge (ADB), který usnadňuje komunikaci mezi zařízeními se systémem Android a osobním počítačem (35). Tato komunikace probíhá prostřednictvím USB nebo přes Wi-Fi, pokud to zařízení podporuje (35). Společně se při instalaci ADB instaluje i nástroj fastboot, který funguje pouze v režimu bootloader/fastboot a umožňuje přeflashovat systémové oddíly v zařízení. To je především potřebné při instalovaní nového operačního systému (36). Poté pro správnou komunikaci s nástrojem ADB je nutno aktivovat vývojářský režim a ADB debugging na zařízení TicWatch (18). U některých osobních počítačů s operačním systémem Windows je taktéž nutné nainstalovat či aktualizovat USB Android ovladač, obvykle se tento problém projevuje špatnou detekcí android zařízení. Následující návod popisuje podrobně přípravu k instalaci NetHunter.

3.4.1.1 Návod na povolení vývojářského režimu a ADB debugging

1) Na zapnutém zařízení TicWatch přejděte do hlavního menu a poté do nastavení.

2) Následně přejděte do systému a klikněte na „About“.

3) Z výběru klikněte desetkrát na „Build number“.

4) V hlavní nabídce nastavení se objeví nové nastavení pod názvem „Developer options“, klikněte na tuto možnost a zapněte funkci „ADB debugging“

5) Restartujte zařízení

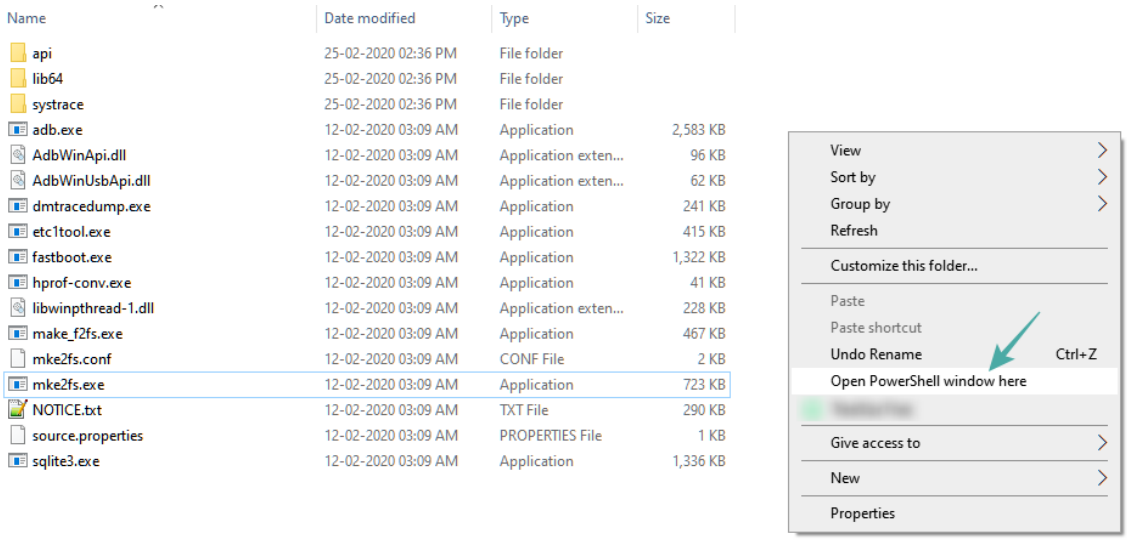
3.4.1.2 Návod k instalaci ADB a Fastboot

1) Stáhněte si nejnovější „Platform tools“ nástroj od oficiálního distributora je dostupný ze zdroje: https://developer.android.com/tools/releases/platform-tools

2) Rozbalte obsah složky „platform-tools.zip“ na libovolné umístění na lokálním pevném disku.

3) Poté přejmenujte rozbalenou složku na „adb“ a přemístěte ji do kořenového adresáře „C:\“

4) Otevřete soubor pod názvem „mke2fs.exe“ pomocí programu PowerShell podle návodu na obrázku (Obrázek 3.9).

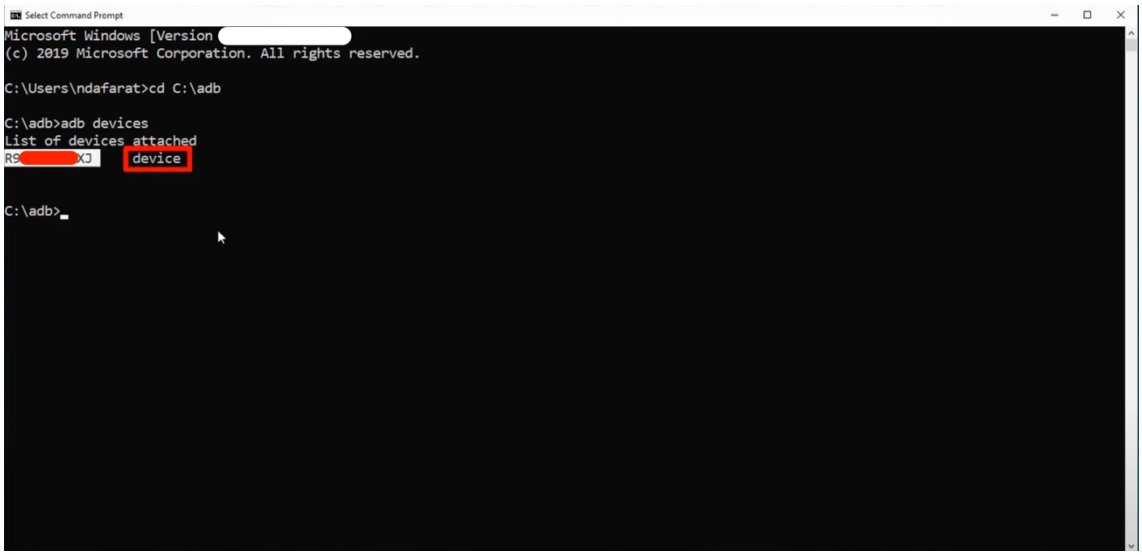


Obrázek 3.9 Návod na otevření souboru "mke2fs.exe". Zdroj: *(36)*

5) Spusťte příkaz

6) Pro ověření správné funkčnosti ADB zapněte příkazový řádek (CMD) a připojte zařízení TicWatch do počítače pomocí datového kabelu. Po připojení zařízení se objeví na zařízení okno s povolením ADB debugging, povolte. Zadejte příkaz „cd C:\“ a potvrďte stisknutím Enter. Tento příkaz otevře složku „adb“ s nástrojem. Následně zadejte příkaz „adb devices“ a potvrďte.

7) Zobrazí se seznam s názvem připojeného zařízení. Na ukázkovém obrázku (Obrázek 3.10) je správný postup.



Obrázek 3.10 Ukázkový postup ověření správně instalace ADB. Foto: Snímek obrazovky. Zdroj: Snímek obrazovky (CMD)

3.4.1.3 Návod k instalaci ovládače Android

Pokud zařízení TicWatch Pro nebylo rozpoznáno pomocí ADB je nutno nainstalovat či aktualizovat Android ovladač. Tento ovladač je oficiálně k dispozici na stránkách Developer Android (37). Po stažení rozbalte archiv zip a přejdete do správce zařízení. Zde je podrobný návod na instalaci ovladače:

1) Po stažení rozbalte archiv zip a přejdete do správce zařízení skrze vyhledávání ve Windows.

2) Najděte v seznamu neznámý zařízení a v této sekci klikněte pravým tlačítkem na zařízení „Android“. Poté klikněte na „Aktualizovat ovladač“

3) Následně vyberte druhou možnost „Vyhledat ovladač v počítači“.

4) Zvolte opět druhou možnost pod názvem „Vybrat ovladač ze seznamu“.

5) Poté zvolte „Z disku“ a najděte staženou složku.

6) Vyberte v složce soubor pod názvem „android_winusb.inf“ a potvrďte.

7) Zobrazí se seznam ovladačů, který je možný nainstalovat. Vyberte „Android ADB Interface“ a klikněte na „Další“.

8) Poté se zobrazí okno s potvrzením instalace, klikněte na „instalovat“.

3.4.1.4 Stažení potřebných souborů k instalaci operačního systému NetHunter

K instalaci operačního systému Nethunter je potřeba stáhnout několik souborů z oficiální stránky distributora (18). První požadovaný soubor je „vbmeta.img“, který slouží k deaktivaci kontroly integrity. Tato kontrola a bootovací obraz, zajišťuje, že se na konkrétním zařízení pomocí digitálního klíče zapínal pouze konkrétní operační systém. Dalším souborem je „recovery.img“ tento soubor umožní po jeho instalaci vstoupit do Recovery mode (obnovovací režim) (38). Existují dva dostupný soubory pro obnovení pod názvem „Rover“ (pro LTE verzi hodinek) a „Rubyfish“ (pro GPS verzi), proto je třeba zkontrolovat před stažením souboru, o který konkrétní typ verze TicWatch se jedná. Následující soubor pod názvem „OneOS.zip“ slouží k nahrání čistého operačního systému a má taktéž dvě dostupné verze Rover a Rubyfish. Nový operační systém se instaluje bez aplikací od výrobce hodinek. Tyto aplikace neovlivňují využití penetračního systému, avšak pokud by uživatel chtěl i nadále využívat tyto hodinky jako chytré je nutné si stáhnout soubor „MobvoiAPPS.zip“. NetHunter vyžaduje přístup k systémovým složkám a k procesům, a proto je nutné na nový operační systém nainstalovat root oprávnění pomocí souborů „Magisk.zip“ a „Magisk.apk“. Po instalaci Magisk je nezbytné provést deaktivaci ochrany proti neoprávněným úpravám systému pomocí souboru „disabler.zip“. Poté zbývá už jen poslední soubor s instalačním obrazem sytému pod názvem „NetHunter.zip“. Níže je uvedená přehledná tabulka (Tabulka 5) s potřebnými soubory.

Tabulka 5 Přehledná tabulka s instalačními soubory

Tabulka souborů
vbmeta.img
recovery.img
Rubyfish
OneOS.zip
MobvoiAPPS.zip
Magisk.zip
Magisk.apk
disabler.zip
NetHunter.zip

3.4.2 Návod k instalaci operačního systému NetHunter

1) Spusťte příkazový řádek a poté aktivujte ADB pomocí příkazu „cd C:\“.

2) Připojte zařízení TicWatch k počítači.

3) Přepněte hodinky do režimu bootloader pomocí příkazu „adb reboot bootloader a stiskněte Enter. Možné je též využít alternativní způsob přepnutí do tohoto režimu pomocí stisknutí a podržení dvou bočních tlačítek.

4) Vyčkejte, než se zařízení restartuje a zobrazí se menu s nápisem „START“ viz obrázek (*Obrázek 3.11*).

Obrázek 3.11 Fastboot mode. Zdroj: *(39)*

5) Zadejte do příkazového řádku „fastboot oem unlock“. Tento příkaz odemkne bootloader a umožní instalaci alternativního operačního systému.

6) Následně potvrďte odemčení bootloaderu na zařízení TicWatch pomocí stisknutí a dlouhého podržení dolního bočního tlačítka.

7) Vyčkejte, než se zařízení restartuje a spustí se operační systém. Poté znovu aktivujte vývojářský režim a ADB Debugging podle návodu v přípravě.

8) Restartujte zařízení a opakujte třetí krok. Po načtení bootloaderu se ujistěte, že se v posledním řádku se objevilo „DEVICE STATE – unlocked“.

9) Zadejte do příkazového řádku „--disable-verity --disable-verification flash vbmeta C:\cesta k souboru vbmeta\vbmeta.img“. Tento příkaz provede nahrání bootovacího obrazu a zároveň vypne kontrolu integrit.

10) Nahrajte do zařízení recovery.img pomocí příkazu „fastboot flash recovery C:\ cesta k souboru \ recovery.img“.

11) Přejděte do recovery módu v menu bootloaderu pomocí bočních tlačítek (horní tlačítko odpovídá za výběr, spodní za potvrzení).

12) Po načtení Recovery módu se zobrazí dialogové okno s povolením zápisu do zařízení. Povolte kliknutím na tlačítko „Allow Modifications“. Následně se dostanete do hlavního menu recovery módu viz obrázek (Obrázek *3.12*).

Obrázek 3.12 Hlavní menu Recovery Mode. Foto: Autor

13) Vyberte v recovery módu volbu „Wipe“ poté v právem dolním rohu klikněte na šipku a zvolte „Format Data“. Následně vyskočí potvrzovací dialogové okno, které potvrdíte vepsáním „yes“ pomocí klávesnice.

14) Vraťte se zpět do hlavního menu recovery módu pomocí tlačítka „domů“. Vyberte z nabídky volbu „Reboot“ a následně zvolte „Recovery“. Poté se zařízení restartuje zpět do recovery módu.

15) V hlavní nabídce vyberte volbu „Install“ poté zvolte „ADB sideload“. Po zvolení této volby zařízení čeká na nahrání instalačního souboru.

16) Nahrajte nový operační systém OneOS pomocí příkazu „adb sideload C:\ cesta k souboru \oneos.zip“. Vyčkejte na dokončení instalace a poté restartujte zařízení pomocí volby reboot.

17) Nahrajte výchozí aplikace Mobvoi opakováním kroku 15) a příkazem „adb sideload C:\ cesta k souboru \MobvoiAPPS-TWP3_full.zip“. Stejně tak vyčkejte a restartujte zařízení.

18) Stejně tak nahrajte aplikaci Magisk příkazem „adb sideload C:\ cesta k souboru \Magisk-v24.3.zip“.

19) Nahrajte deaktivaci ochrany systému proti změnám pomocí příkazu „adb push C:\ cesta k souboru \disabler.zip /sdcard/“.

20) Přejděte v recovery módu do volby „Install“ a poté zvolte „Install Zip“, a zvolte soubor z kroku 19).

21) Vypněte a restartujte zařízení pomocí volby „Reboot“ a následně „System“.

22) Proveďte počáteční nastavení hodinek (spárování s telefonem).

23) Aktivujte vývojářský režim a ADB Debugging podle návodu v přípravě.

24) Přepněte hodinky do Bootloaderu podle kroku 3) a zapněte recovery mód.

25) Nainstalujte Magisk v „Install ADB“ příkazem „adb install C:\ cesta k souboru \Magisk-v24.3.apk“.

26) Restartujte zařízení pomocí „Reboot System“.

27) Po zapnutí zařízení se v seznamu aplikací objeví „Magisk Manager“ klikněte na ní a ujistěte se, že v aplikaci je nainstalován Magisk a je k dispozici SuperUser podle obrázku (Obrázek *3.13*).

Obrázek 3.13 Magisk Manager. Foto: Autor

28) Přepněte zařízení do bootloaderu zpětně podle kroku 3) a zapněte recovery mód.

29) Nainstalujte Nethunter v „Install ADB“ pomocí příkázu „adb sideload C:\ cesta k souboru\nethunter-2022.2b-ticwatchpro-wearos-kalifs-nano.zip“

30) Restartujte zařízení pomocí „Reboot System“.

31) Při načítaní operačního systému se zobrazí logo kali-linux viz obrázek (Obrázek *3.14*) a po zapnutí se objeví v seznamu aplikací aplikace NetHunter.

Obrázek 3.14 Bootování operačního systému NetHunter. Foto: Autor

32) Otevřete aplikaci Magisk a povolte root oprávnění podle obrázku (Obrázek *3.15*) pro aplikace „NetHunter“ a „NetHunterTerminal“ v nabídce SuperUser.

Obrázek 3.15 Root oprávnění. Foto: Autor

33) Vše je nainstalováno a připraveno k použití.

3.5 Návod k použití TicWatch s NetHunter

Po úspěšné instalaci operačního systému NetHunter je zařízení plně připraveno k testování sítě. Zařízení je schopné provádět útok na zranitelnost WPS pomocí hrubou silou (BruteForce) a útoku zmáčknutím tlačítka „WPS“. Při této volbě je nutno při útoku zmáčknout tlačítko „WPS“ na routeru. Dále je popsán návod pro testování obou možností útoku.

3.5.1 Útok hrubou silou / Tlačítkem

Útok hrubou silou spočívá v opakovaném testováním všech možných kombinací PIN kódu WPS zabezpečení. WPS není tak dobře zabezpečený a pro jeho prolomení stačí pouze 11000 kombinací. Zde je návod:

1) Zapněte aplikaci pod názvem „NetHunter“.

2) Klikněte do levého dolního rohu menu baru podle šipky na obrázku (*Obrázek 3.16*). Systém není tak dobře optimalizovaný na hodinky. Nachází se tam hlavní menu.

Obrázek 3.16 Znázornění menu. Foto: Autor

3) V sekci menu přejděte do sekce „WPS Attacks“ viz obrázek (*Obrázek 3.17*).

Obrázek 3.17 Sekce "WPS Attacks". Foto: Autor

4) Poté se otevře menu pro testování WPS. Pomocí tlačítka „SCAN FOR WPS ROUTERS“ proveďte skenování okolních Wi-Fi sítí.

5) Zobrazí se název nejbližší dostupné Wi-Fi sítě. Klikněte na její název, pokud chcete zvolit jinou Wi-Fi síť.

6) Přejděte do nižší sekce a zde jsou k dispozici dvě varianty útoku. První varianta je útok hrubou silou, zvolte dvě volby „Pixie Dust“ a „Pixie Force“ podle obrázku (*Obrázek 3.18*). Druhou variantou je útok tlačítkem „WPS Button“. Poté potvrďte útok tlačítkem „LAUNCH ATTACK“.

Obrázek 3.18 Volba útoku. Foto: Autor

7) Vyčkejte, než se otevře terminál a spustí se útok na WPS sít.

8) Pokud útok byl úspěšně proveden, zobrazí se v terminálu: „WPS PIN“, “WPA PSK“ a „AP SSID“. Tímto bylo heslo úspěšně prolomeno. Při neúspěšném útoku opakujte návod od kroku 4).

3.6 Úlohy pro studenty

Studenti si v rámci dvou cvičení vyzkouší dvě úlohy na testování bezdrátové sítě podle sestavených manuálů. Otestují zranitelnost Wifi sítě penetračním systémem v uzavřeném prostoru pomocí hodinek DEAUTHER Watch a dronu. Tato úloha by měla studentům poukázat na jednoduchost zranitelnosti a nepodstatnost nepřístupnosti. Vzhledem k tomu, že potenciální útočník se dokáže dostat pomocí tohoto systému i do míst s obtížným přístupem.

Druhá úloha spočívá v prolomení WPS PINU prostřednictvím chytrých hodinek s operačním systémem Nethunter. Studenti si též vyzkouší rozsáhlou instalaci Nethunteru na standartních hodinkách TicWatch podle manuálu. Musí se jednat o úplné nové hodinky. Opětovnou instalaci není možné provést na hodinkách, které již mají provedenou instalaci NetHunter. Tato úloha by měla zdůraznit nenápadnost útoku, jelikož se toto penetrační zařízení zároveň chová na pohled jako obyčejné hodinky. Útočník v případě útoku dokáže kdykoliv zneužít systém pro penetraci sítě. Studenti provedou dva typy útoků podle návodu.

4 Testování

Výsledkem testování sytému je provést vzdálenou penetraci Wi-Fi sítě v neveřejné a bezletové zóně. Před samotným testováním proběhlo samostudium v oblastech letecké bezpečnosti, obecných znalostí bezpilotních systému, předpisů týkajících se letectví a provozních postupů. Poté proběhla registrace pilota a absolvování online zkoušky pro pilota bezpilotního systému v podkategorii A1 a A3. Následovala příprava veškerého vybavení zařízení, výběr místa a samotné testování.

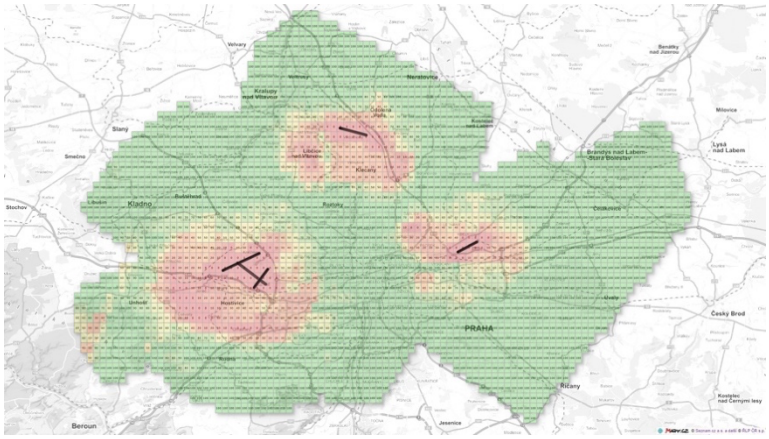
4.1 Příprava sytému

Testovací systém se skládá z bezpilotního systému DJI Mini Pro, penetračního zařízení DEATHER Watch, mobilních telefonu pro vysílaní a příjímání přístupového bodu, tabletu pro připojení k penetračnímu zařízení viz obrázek (*Obrázek 4.1*). K bezpilotnímu systému bylo připevněno penetrační zařízení pomocí řemínku a otestováno vzlétání a přistání ve vnitřních prostorech. Poté proběhla úspěšná penetrace sítě pomocí DEATHER Watch ve vnitřních prostorech. Chytrý telefon (iPhone 13 Pro) vysílal přístupový bod a druhý telefon (iPhone 6s) byl připojený k této síti. Tablet (iPad Pro) byl vzdáleně připojen k penetračnímu zařízení a prováděl útok „Deauth“ (odpojení všech zařízení) na vytvořenou Wi-Fi sít.

Obrázek 4.1 Penetrační systém. Foto: Autor

4.2 Výběr místa

Důležité bylo vybrat neveřejné a bezletové místo pro penetrační testování. Řízení letového provozu České republiky poskytuje online mapu bezletových zón dronview. Pomocí dronview a gridové mapy letišť viz obrázek (*Obrázek 4.2*), která je dostupná na stránce „letejtezodpovedne.cz“ byla vybrána oblast poblíž Prahy. Poté byla tato oblast prozkoumaná autem a vybrána neveřejná louka pro testování.

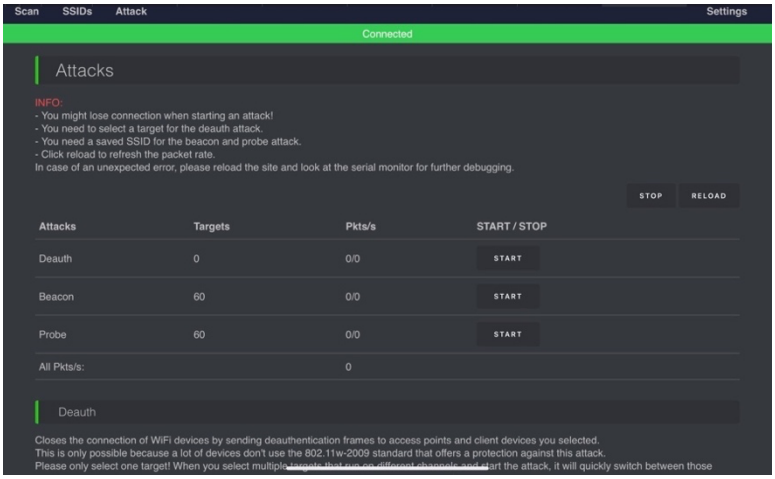


Obrázek 4.2 Gridová mapa Praha Ruzyně. Zdroj: Snímek obrazovky

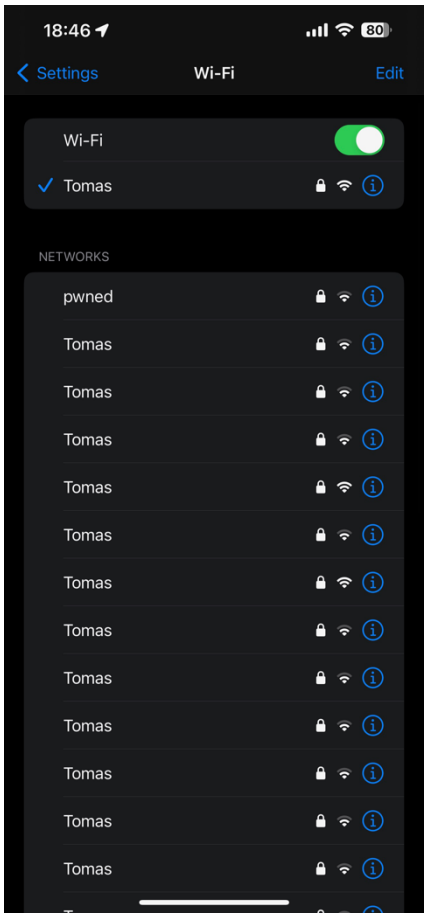
4.3 Penetrační testování systému

Testování probíhalo na vybrané louce. Testovaný telefon společně s přístupovým bodem se nacházely přibližně 15 metrů od penetračního systému. Tablet se připojil vzdáleně k síti DEATHER Watch, které se nacházely na bezpilotním systému poblíž. Poté společně s dronem vzlétl na poloviční vzdálenost mezi tabletem a cílovou Wi-Fi síti viz obrázek (Obrázek *4.3*). Následně pomocí webového rozhraní na tabletu (Obrázek *4.4*) připojeného k DEATHER Watch probíhal úspěšný útok (Obrázek *4.5*) „Deauth“ a „Beacon“ (zaplavení falešných SSID).

Obrázek 4.3 Penetrační systém: Dron a DEATHER Watch. Foto: Autor



Obrázek 4.4 Webové rozhraní serveru DEAUTHER Watch. Zdroj: Snímek Obrazovky



Obrázek 4.5 Testování útoku Beacon. Zdroj: Snímek obrazovky

4.4 Penetrační testování zařízení TicWatch Pro

Zařízení TicWatch nenabízí možnost vzdáleného ovládání, a tím pádem je zbytečné ho připevňovat k dronu. Testování proto proběhlo ve vnitřním prostoru a na starším routeru TP-LINK TL-WR841N. Byl proveden úspěšný útok na prolomení hesla a poté na reset WPS viz obrázek (Obrázek 4.6). Hodinky prolomily heslo během pár vteřin, avšak na krátkou vzdálenost. Při testování na větší vzdálenost ve vedlejší místnosti od routeru se hodinky zacyklily na připojení (connecting) a nedokázaly prolomit heslo.

Obrázek 4.6 Prolomení WPS hesla na zařízení TicWatch. Zdroj: Autor

5 Diskuse

V dnešní době je technologie Wi-Fi nezbytnou součástí našeho života a v drtivé většině případů se lidé připojují k neznámé síti a na zabezpečení už nemyslí. Příkladem je veřejná Wi-Fi síť v restauracích, kavárnách a veřejných prostorech. Potenciální útočníci mohou v takových místech například ukrást citlivé informace s využitím nenápadných prostředků, jako jsou mobilní telefony či dokonce chytré hodinky. Tímto by mohli způsobit výraznou škodu nejen na duševním ale i finančním vlastnictví. Testování dokonce prokázalo, že se útočníci ani nemusí nacházet v blízkém okolí.

Myslím si, že hlavním problémem je především zanedbaní vzdělání běžných uživatelů. Problematika ochrany bezdrátové sítě obvykle nebývá zahrnuta ve výuce, a to ani na středních či základních školách se zaměřením na IT. Aby se povědomí o těchto a podobných bezpečnostních mezerách v budoucnu zvýšilo, je nutné žáky a studenty na tyto mezery v bezpečnosti upozornit a vzdělávat je v otázkách bezpečnosti. Návody k praktickým cvičením vytvořené v této práci k tomu tvoří ideální základ. Byly navrženy tak, aby byly praktické a zajímavé, aby vzbudily co největší zájem o téma, ale také aby předaly co nejvíce znalostí. Navržený systém lze ve výuce využít, avšak použití zařízení TicWatch Pro má nevýhodu v tom, že pro každou novou instalaci operačního systému je nutné zakoupit nové chytré hodinky. V závislosti na časových možnostech, předchozích technických znalostech a finančních možnostech škol a univerzit lze tyto úlohy provádět jednotlivě či po sobě. Úlohy a postupné instrukce vytvořené v této práci mohou být vyučujícím rozšířeny nebo upraveny v závislosti na účelu výuky a předchozích technických znalostech. Úlohy působivě demonstrují zranitelnost Wi-Fi sítí a lze je tak provádět v jakékoli vyučovací hodině v oblasti IT bezpečnosti.

6 Závěr

V první části bakalářské práci byla provedena rešerše, která obsahuje seznámení s penetračním testováním, architekturou, standarty a problematikou ochrany bezdrátových Wi-Fi sítí. V kapitole penetrační testování jsou popsány klíčové pojmy a typy testovaní. Následně jsou stručně porovnány standardy IEEE 802.11 a popsána architektura WLAN. Sekce problematiky ochrany se zabývá rozdíly a zranitelností jednotlivých protokolů zabezpečení.

V další části byl proveden průzkum trhu penetračních zařízení a transportních nástrojů. Byly zvoleny dvě varianty testovacích zařízení, jedná se o hardwarové zařízení přímo určené k testování a software pro chytré hodinky. Pro transport testovacího zařízení byla zvolena letecká přeprava. Konkrétněji se jedná o bezpilotní letoun (dron). Byl sestaven návrh jednotlivých zařízení a krátký popis technických informací. Bezpilotní systém v České republice může provozovat jen osoba, která složila speciální zkoušku pilota. Na základě toho proběhlo samostudium a poté absolvování zkoušky z teoretických znalostí.

Po sestavení návrhů penetračního systému nastala implementace. Výroba krytu dokovací stanice pomocí 3D tiskárny pro instalaci penetračního softwaru a sestavení výrobního návodu. Následovala samotná rozsáhlá instalace operačního systému na chytré hodinky a sepsání podrobného manuálu pro studenty.

Poté proběhlo úspěšné testování penetračního systému (penetrační hardwarové zařízení a dron) na neveřejném a legálním prostoru pro dron. Penetrační zařízení pomocí bezpilotního systému se přiblížilo k cílovému přístupovému bodu a provedlo vzdálený útok. Bylo taktéž realizováno i úspěšné testování hodinek s operačním systémem NetHunter na starším routeru ve vnitřním prostoru. Následně byly sepsány srozumitelné návody obou zařízení.

Seznam použité literatury

1. **Whitaker, Andrew a Newman, Daniel.** *Penetration Testing and Network Defense.* Indianapolis : Cisco Press, 2006. ISBN: 1-58705-208-3.

2. **Cesnet.** Penetrační testování – co to je, jak na ně. *cesnet.* [Online] [Citace: 15. Březen 2023.] https://hsoc.cesnet.cz/_media/cs/dokumenty/tech/penetracni_testovani-summary.pdf.

3. **Pocketlabs.** Black-Box vs Grey-Box vs White-Box Penetration Testing. *Packetlabs.* [Online] 19. Duben 2022. [Citace: 15. Březen 2023.] https://www.packetlabs.net/posts/types-of-penetration-testing/.

4. **Klement, Milan.** *Technologie bezdrátových sítí.* Olomouc : Univerzita Palackého v Olomouci, 2017. ISBN: 978-80-244-5156-5.

5. **Danel, Eve.** Wi-Fi 6E Standard and Channels – 802.11ax Operation in the 6 GHz Band. *LITEPOINT.* [Online] 10. Listopad 2020. [Citace: 17. Březen 2023.] https://www.litepoint.com/blog/wi-fi-6e-standard-and-channels/.

6. **ASM.** Vývoj WiFi standardů až k IEEE 802.11ac. *ASM.* [Online] [Citace: 18. Březen 2023.] https://www.asm.cz/cs/faq/1840-vyvoj-wifi-standardu-az-k-ieee-802-11ac.

7. **Neznámý.** IEEE 802.11. *wifi unas.* [Online] [Citace: 18. Březen 2023.] http://wi-fi.unas.cz/ieee-802-11.php.

8. **Irei, Alissa.** Wireless security: WEP, WPA, WPA2 and WPA3 differences. *TechTarger.* [Online] Prosinec 2022. [Citace: 2. Duben 2023.] https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2.

9. **Jandura, Martin.** The standard for wireless transfer of data and IEEE 802.11x, Bakalářská práce. *dspace.* [Online] 2007. [Citace: 5. Duben 2023.] https://dspace.tul.cz/bitstream/handle/15240/47510/V_09507_Mb.pdf?sequence=1&isAllowed=y.

10. **Navrátil, Lukáš.** Zabezpečení bezdrátových sítí WiFi, Bakalářská práce. *dspace.* [Online] 2011. [Citace: 5. Duben 2023.] https://dspace.tul.cz/bitstream/handle/15240/9597/bc_18253.pdf?sequence=1&isAllowed=y.

11. **KULÍŘ, Bc. TOMÁŠ.** ANALÝZA ZABEZPEČENÍ A AUTENTIZACE BEZDRÁTOVÝCH SÍTÍ, DIPLOMOVÁ PRÁCE. *core ac.* [Online] 2011. [Citace: 5. Duben 2023.] https://core.ac.uk/download/pdf/30297793.pdf.

12. *Research on WiFi Penetration Testing with Kali Linux.* **Lu, He-Jun a Yu, Yang.** místo neznámé : Hindawi, 2021, Sv. 2021. 1076-2787.
13. **bezpečnost, Národní úřád pro kybernetickou a informační.** KRACK - zranitelnost protokolu WPA2 umožňuje čtení šifrovaných dat. *nukib.* [Online] 16. říjen 2017. [Citace: 15. Duben 2023.] https://nukib.cz/cs/infoservis/hrozby/1459-krack-zranitelnost-protokolu-wpa2-umoznuje-cteni-sifrovanych-dat/.
14. *Anticipating WPS PIN Vulnerability to Secure Wireless Network.* **Rianto, Indra Dwi.** 2, místo neznámé : ComTech: Computer, Mathematics and Engineering Applications, 2013, Sv. 4. ISSN: 2087-1233.
15. **LIESKOVAN, TOMÁŠ.** MODERNÍ TRENDY V ZABEZPEČENÍ WI-FI SÍTÍ STANDARDU IEEE 802.11, Bakalářská práce. *dspace.* [Online] 2015. [Citace: 5. Duben 2023.] https://dspace.vutbr.cz/bitstream/handle/11012/41351/final-thesis.pdf?sequence=-1.
16. **Stankovic, Strahinja.** How To Perform A Wireless Penetration Test. *PURPLESEC.* [Online] [Citace: 25. Březen 2023.] https://purplesec.us/perform-wireless-penetration-test/.
17. **Lin, Travis.** DSTIKE. *DSTIKE.* [Online] [Citace: 25. Březen 2023.] https://dstike.com/products/dstike-deauther-watch-v3.
18. **Limited, OffSec Services.** Kali Linux Documentation. *Kali Linux.* [Online] [Citace: 20. Duben 2023.] https://www.kali.org/docs/nethunter/installing-nethunter-on-the-ticwatch-pro3/.
19. **Neznámý.** Fruugo. *Fruugo.* [Online] [Citace: 25. Březen 2023.] https://img.fruugo.com/product/1/47/475233471_max.jpg.
20. **Mtoolstec, Shop.** Shop Mtoolstec. *Shop Mtoolstec.* [Online] [Citace: 25. Březen 2023.] https://shop.mtoolstec.com/product/deauther-watch-v2.
21. **Enrique.** Mobvoi TicWatch Pro 3 GPS review. *GSMArena.* [Online] 6. Prosinec 2020. [Citace: 10. Duben 2023.] https://www.gsmarena.com/mobvoi_ticwatch_pro_3_gps_review-news-46538.php.
22. **Neznámý.** Chytré hodinky TicWatch Pro 3 GPS. *okay.* [Online] [Citace: 30. Březen 2023.] https://www.okay.cz/products/chytre-hodinky-ticwatch-pro-3-gps-cerna-pouzite-neopotrebene-zb?variant=39998691344426&gclid=CjwKCAjw04yjBhApEiwAJcvNoSyB7ukJEHIQVI9_3G_KuvvooYzNo1DnIx-0MgU6DTGJKePvM2Mk6xoCu8oQAvD_BwE.

23. **bernarbernuli.** How to make a homemade charging and data cable for Ticwatch Pro 3 (easiest method) . *Reddit.* [Online] Srpen 2022. [Citace: 15. Duben 2023.] https://www.reddit.com/r/WearOS/comments/wpuegq/guide_how_to_make_a_homemade_charging_and_data/.
24. **Re4son, yesimxev.** Kali. *Kali.* [Online] [Citace: 27. Březen 2023.] https://www.kali.org/docs/nethunter/.
25. **danionescu.** RC Car Hack With Android And Arduino. *hackster.* [Online] 29. Červenec 2017. [Citace: 30. Duben 2023.] https://www.hackster.io/danionescu/rc-car-hack-with-android-and-arduino-d31a95.
26. **AUFRANC, JEAN-LUC.** Review of micro:bit XGO Robot Kit – An educational robot dog with a Bluetooth joystick. *CNX SOFTWARE – EMBEDDED SYSTEMS NEWS.* [Online] 7. Březen 2023. [Citace: 20. Duben 2023.] https://www.cnx-software.com/2023/03/07/review-of-microbit-xgo-robot-kit-an-educational-robot-dog-with-joystick/.
27. **ATHERTON, KELSEY D.** Researchers Put A Tiny Computer On A Drone To Make It A Hacking Machine. *POPULAR SCIENCE.* [Online] 29. Červenec 2016. [Citace: 20. Duben 2023.] https://www.popsci.com/researchers-put-tiny-computer-on-drone-to-make-hacking-machine/.
28. **DJI.** DJI Mini 2 SE. *DJI.* [Online] [Citace: 7. Duben 2023.] https://www.dji.com/cz/mini-2-se.
29. **Neznámý.** Dron DJI Mini 3 Pro. *DRONPRO.* [Online] [Citace: 7. Duben 2023.] https://dronpro.cz/dron-dji-mini-3-pro-dji-rc.
30. —. Dron Autel EVO Nano+ Standard Bundle. *DRON PRO.* [Online] [Citace: 7. Duben 2023.] https://dronpro.cz/dron-autel-evo-nano-standard-bundle-cerveny.
31. **letectví, Úřád pro civilní.** Základní informace k regulačnímu rámci EU pro bezpilotní systémy. *caa.* [Online] [Citace: 25. Duben 2023.] https://www.caa.cz/provoz/bezpilotni-letadla/zakladni-informace-k-regulacnimu-ramci-eu-pro-bezpilotni-systemy/.
32. **letectví, Úřad pro civilní.** Školicí materiál ÚCL ve formě FAQ - nejčastěji kladených dotazů k problematice. *CAA.* [Online] [Citace: 25. Duben 2023.] https://www.caa.cz/wp-content/uploads/2022/12/FAQ-DRONES_CS.pdf?cb=9fed2ca656703560382d2ecaafee3930.
33. —. Pilot bezpilotního systému. *caa.* [Online] [Citace: 26. Duben 2023.] https://www.caa.cz/provoz/bezpilotni-letadla/pilot-bezpilotniho-systemu/.

34. **Technologies, Spacehuhn.** Blog spacehuhn. *Blog spacehuhn.* [Online] [Citace: 27. Březen 2023.] https://blog.spacehuhn.com/deauther-oled-interface.
35. **Project, The LineageOS.** LineageOS Wiki. *LineageOS Wiki.* [Online] [Citace: 20. Duben 2023.] https://wiki.lineageos.org/adb_fastboot_guide.
36. **Shivam.** How to Install ADB and Fastboot on Windows: All the methods and help! *Nerdschalk.* [Online] [Citace: 20. Duben 2023.] https://nerdschalk.com/how-to-install-adb-and-fastboot/.
37. **Google, Společnost.** Get the Google USB Driver. *Android Developer.* [Online] [Citace: 21. Duben 2023.] https://developer.android.com/studio/run/win-usb.
38. —. Recovery Images. *Android Open Source Project.* [Online] [Citace: 20. Březen 2023.] https://source.android.com/docs/core/architecture/bootloader/recovery-images.
39. **Neznámý.** HardReset.info: Jak obnovit tovární nastavení MOBVOI TicWatch Pro 3 GPS? *HARDRESET.* [Online] [Citace: 20. Březen 2023.] https://www.hardreset.info/cs/devices/mobvoi/mobvoi-ticwatch-pro-3-gps/obnoveni-tovarniho-nastaveni/.
40. **Google, Společnost.** Android Verified Boot 2.0. *Android GoogleSource.* [Online] [Citace: 21. Duben 2023.] https://android.googlesource.com/platform/external/avb/+/master/README.md.