**OBOR**

**18-20-M/01 INFORMAČNÍ TECHNOLOGIE**

**ŠVP: Správa sítí a IT bezpečnost**

**MATURITNÍ PROJEKT**

TÉMA PRÁCE

**Bezpečnost v informačních technologiích**

2024/2025 Filip Struhár

**PROHLÁŠENÍ**

Prohlašuji, že jsem svou maturitní práci vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, SW, atd.) uvedené v seznamu.

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).

V Praze dne XX. X. 2025 ……………………………………

podpis

**PODĚKOVÁNÍ**

Na prvním místě bych chtěl poděkovat mému vedoucímu práce panu Jiřímu Šilhánovi.

Rovněž bych rád poděkoval všem dalším učitelům, kteří mi svými připomínkami a radami pomohli během vypracovávání této práce. Jejich pomoci si velmi vážím. Na závěr bych chtěl poděkovat své rodině za jejich morální podporu a porozumění.**ANOTACE**

|  |  |
| --- | --- |
| Jméno autora | Filip Struhár |
| Název maturitní práce | Simulace kybernetického útoku |
| Rozsah práce | Počet stran práce ve formátu (např. 165 s. + 50 s. příloh) |
| Školní rok vyhotovení | 2024/2025 |
| Škola | Střední průmyslová škola na Proseku |
| Vedoucí práce | Jiří Šilhán |
| Využití práce | Penetrační testovaní wifi sítí, skenování dostupných wifi sítí a jejich parametrů, a bezpečností auditování. |
| Abstrakt | Práce je zaměřena na bezpečnost bezdrátových sítí wifi a návrhu jejich obrany. |
| Klíčová slova | Linuxový nástroj, penetrační testování wifi, bezpečnost wifi, python |

**ANNOTATION**

|  |  |
| --- | --- |
| Autor | Filip Struhár |
| Title of graduation work | Simulation of a cyber attack |
| Extend | Např. 165 p. + 50 p. of appendices |
| Academic year | 2024/2025 |
| School | Střední průmyslová škola na Proseku |
| Supervisor | Jiří Šilhán |
| Application | Penetration testing of wifi networks, scanning of available wifi networks and their parameters, and security auditing. |
| Abstrakt | The project is focused on the security of wifi wireless networks and their defense design. |
| Key words | Linux tool, wifi penetration testing, wifi security, python |
|  |  |

**Obsah**

[1 ÚVOD 9](#_Toc191228571)

[2 Zabezpečení wifi 10](#_Toc191228572)

[2.1 Jak funguje wifi? 10](#_Toc191228573)

[2.2 Šifrovací metody 11](#_Toc191228574)

[2.2.1 WEP (Wired Equivalent Privacy) 11](#_Toc191228575)

[2.2.2 WPA (Wi-Fi Protected Access) 12](#_Toc191228576)

[2.2.3 WPA2 13](#_Toc191228577)

[2.2.4 WPA3 13](#_Toc191228578)

[2.3 Enterprise autentizace 14](#_Toc191228579)

[2.3.1 RADIUS server 14](#_Toc191228580)

[2.4 Zjednodušená autentizace ve WiFi sítích 14](#_Toc191228581)

[2.4.1 WPS (Wi-Fi Protected Setup) 15](#_Toc191228582)

[2.4.2 DPP (Device Provisioning Protocol) 15](#_Toc191228583)

[2.5 Segmentace sítě 16](#_Toc191228584)

[3 Bezpečnostní slabiny WiFi 17](#_Toc191228585)

[3.1 WEP 17](#_Toc191228586)

[3.2 Prolomení 4-Way handshake 18](#_Toc191228587)

[3.2.1 Vyjednání šifrovacích klíčů 18](#_Toc191228588)

[3.2.2 Brute force na handshake 19](#_Toc191228589)

[3.3 WPS 20](#_Toc191228590)

[3.3.1 Brute force 20](#_Toc191228591)

[3.3.2 Pixie dust 20](#_Toc191228592)

[3.4 PMKID 21](#_Toc191228593)

[3.5 Mann In The Middle 22](#_Toc191228594)

[3.5.1 Evil Twin 22](#_Toc191228595)

[3.6 Rogue AP 23](#_Toc191228596)

[3.7 Wifi jamming 23](#_Toc191228597)

[4 Specifikace použitých systémových komponent 24](#_Toc191228598)

[4.1 Systémové specifikace 24](#_Toc191228599)

[4.2 Bezdrátové síťové karty 25](#_Toc191228600)

[4.2.1 Tenda U10 C650 25](#_Toc191228601)

[4.2.2 Mediatek MT7922 25](#_Toc191228602)

[5 Přístupové body 26](#_Toc191228603)

[5.1 Mikrotik RB941-2nDs 26](#_Toc191228604)

[5.2 TP-Link AX23 27](#_Toc191228605)

[5.3 TP-Link WR740N 28](#_Toc191228606)

[6 Konfigurace vývojového prostředí 29](#_Toc191228607)

[6.1 Využívané systémové balíčky 30](#_Toc191228608)

[6.1.1 Make 30](#_Toc191228609)

[6.1.2 Gawk 30](#_Toc191228610)

[6.1.3 Sed 30](#_Toc191228611)

[6.1.4 Iputils 30](#_Toc191228612)

[6.1.5 Iproute2 31](#_Toc191228613)

[6.1.6 Iw 31](#_Toc191228614)

[6.1.7 Python311 31](#_Toc191228615)

[6.1.8 Aircrack-ng 31](#_Toc191228616)

[6.1.9 Hashcat 31](#_Toc191228617)

[6.1.10 Pocl 32](#_Toc191228618)

[6.1.11 Hostapd 32](#_Toc191228619)

[6.1.12 Dhcp-server 32](#_Toc191228620)

[6.1.13 Iptables 32](#_Toc191228621)

[6.1.14 Coreutils 32](#_Toc191228622)

[6.2 Využívané „Hcxtools“ 33](#_Toc191228623)

[6.3 Příprava pythonu 34](#_Toc191228624)

[6.3.1 Virtuální prostředí 34](#_Toc191228625)

[6.3.2 Scapy 35](#_Toc191228626)

[6.3.3 Prettytable 35](#_Toc191228627)

[6.3.4 Psutil 36](#_Toc191228628)

[7 Mechanismy nástroje a instalačního skriptu 36](#_Toc191228629)

[8 Instalace WiFighteru 37](#_Toc191228630)

[9 Použití WiFighteru a jeho rozhraní 39](#_Toc191228631)

[9.1 Nápověda k nástroji 39](#_Toc191228632)

[9.2 Podpříkazy nástroje 40](#_Toc191228633)

[9.3 Rozhraní nástroje 40](#_Toc191228634)

[ZDROJE 43](#_Toc191228635)

[SEZNAM OBRÁZKŮ 46](#_Toc191228636)

# ÚVOD

Práce je zaměřena na penetrační testování bezdrátových sítí wifi a jejich bezpečnostnímu auditování. Je navržena jako linuxový nástroj v terminálu, napsaný v jazyku python pro distribuci OpenSUSE Tumbleweed. Tento nástroj disponuje několika příkazy, které uživateli usnadní práci se bezdrátovými síťovými rozhraními a nástrojem jako takovým, a hlavním příkazem, který spustí nástroj v jednoduchém rozhraní terminálu.

Práce automatizuje a zjednodušuje 4 běžné útoky na bezdrátové sítě, které by za normálních okolností vyžadovali zdlouhavý proces a hlubší znalosti uživatele. Při úspěšně provedeném útoku a následném prolomení hesla generuje nástroj stručné reporty s časovým otiskem, parametry wifi sítě a prolomeným heslem. V některých případech jsou ukládány úspěšně zachycené záznamy komunikace, které jsou pak uživateli dostupné pro prolomení hesla využitím jiných nástrojů. Umožňuje také skenování okolních wifi sítí a získávání jejich parametrů jako například typ zabezpečení, autentifikační metoda a šifrovací algoritmus.

Motivací pro tvorbu této práce byl autorův zájem o hlubší pochopení bezpečnostních slabin wifi a návrhu jejich obrany a také slabý výskyt nástrojů, které by zahrnovaly více wifi útoků zahrnutých do jednoho nástroje s jednoduchým rozhraním a ovládáním.

# Zabezpečení wifi

Wifi je bezdrátová síťová technologie, která umožňuje mnoha zařízením komunikovat mezi sebou a internetem bez nutnosti zdlouhavého a složitého pokládání kabelů. Narozdíl od ethernetového řešení ale zdaleka nedosahuje tak vysokých přenosových rychlostí a spolehlivosti. Tato technologie je definována standardem IEEE 802.11.

## Jak funguje wifi?

Pro nasazení této technologie se používají wifi routery, repeatery a access pointy. K přenosu dat jsou používány rádiové vlny, které jsou vysílány na určitém frekvenčním pásmu. Obvykle se k přenosu využívají pásma 2,4GHz a 5GHz, kde 2,4GHz díky jeho delší vlnové délce poskytuje větší pokrytí a dosah, zatímco 5GHz vyšších přenosových rychlosti. U některých bezdrátových routerů s vyšší cenou se můžeme v dnešní době setkat s pásmem 6GHz. Dalšími důležitými pojmy jsou šířka pásma (20, 40 a 80MHz) a čísla kanálů, která se odvíjejí od frekvenčního pásma. Kanály umožňují vysílačům eliminovat jejich vzájemné rušení. Šířka pásma definuje množství dat, které může být v jednom čase přenášeno. Platí ale pravidlo, že čím vyšší je šířka pásma tím větší šíři kanálů vysílač “zabírá” a ruší. Wifi se dále dělí na různé standardy (Wifi 1 - 802.11b, Wifi 2 - 802.11a, …), které vnímáme jako generace obohacující technologii o vyšší přenosové rychlosti, funkce a pokročilejší bezpečnostní techniky.



Obrázek - Wifi standardy (1)

## Šifrovací metody

Díky tomu, že wifi nevyužívá žádné kabely a signály obsahující data vysílá volně do prostoru, není možné fyzicky zamezit tomu, aby si jakýkoliv náhodný útočník přenášená data zachytil a zpracoval. Kvůli této problematice postupem času začaly vznikat způsoby a techniky, jak uchovat přenášená data po wifi síti v bezpečí.

Šifrovací metody wifi slouží k ochraně přenášených dat před jejich odposlechem, autentifikaci klientů a kontroly integrity dat po přenosu po wifi. V dnešní době jsou známy tyto šifrovací protokoly: WEP, WPA, WPA2, WPA3. Šifrovací protokol WEP je považován za zastaralý a již by se z pohledu bezpečnosti neměl nacházet na žádné wifi síti. Nejbezpečnějším řešením v dnešním době je WPA3 nabízející nejpokročilejší šifrovací algoritmy a zabezpečovací funkce, ale není podporován všemi access pointy. V takovém případě je používán jeho předchůdce WPA2, který je stále široce využíván a je považován za bezpečný.

### WEP (Wired Equivalent Privacy)

První vyvinutou šifrovací metodou pro wifi. K šifrování dat používá RC4 64/128/256bitový klíč, který je sdílený mezi všemi zařízeními v síti, jedná se tedy o statický klíč. Skládá se ze dvou částí - sdíleného klíče (40, 104 nebo 232bitový) a inicializačního vektoru IV (24 bitů).

Inicializační vektor sdíleného klíče je připojen na začátek každého klíče a je vysílán nešifrovaně. Jeho účelem je diverzifikace klíče pro různé datové rámce, bohužel kvůli jeho délce dochází k opakování klíčů při delším používání.

Pro zajištění integrity dat WEP využívá CRC-32 kontrolní součet. Před odesláním dat je stejným RC4 klíčem šifrován takzvaný kontrolní součet (32bitový hash postaven z dat před odesláním), který je u přijímače po dešifrování zkontrolován, zda je totožný a nebyl cestou změněn. Autentizace u tohoto protokolu je pouze jednosměrná a je ověřován pouze klient. Existují dvě metody autentizace, a to „Open system“ autentizace, při které klient žádnou autentizací neprovádí nebo „Shared Key“ autentizace, při které se používá WEP klíč, který může být následně útočníkem z úvodního handshaku snadno získán.

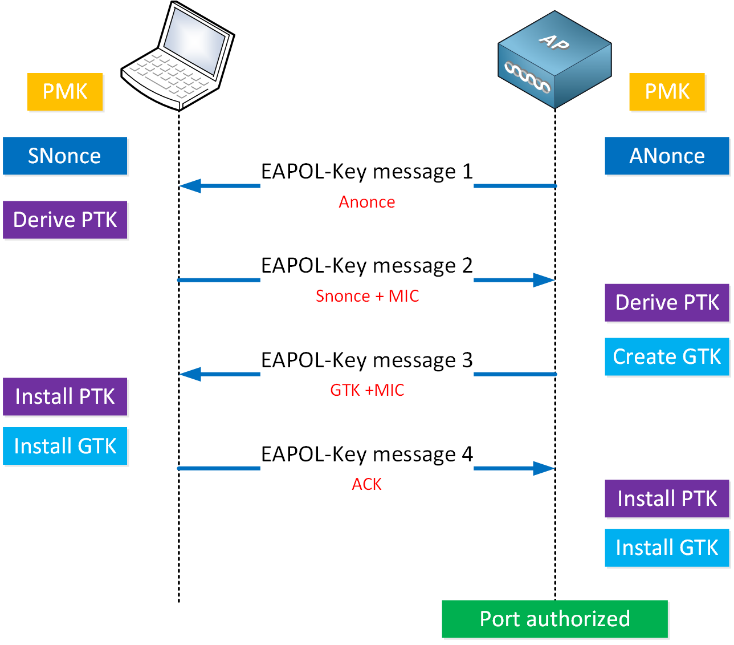
### WPA (Wi-Fi Protected Access)

Využívá k šifrování dat TKIP, který stále používá šifrovací algoritmus RC4 jako jeho základ, ale oproti WEP jsou klíče dynamické, to znamená, že pro každý paket je generován nový 128bitový klíč a v průběhu komunikace je klíč nadále měněn. Což zamezuje, aby byl útočník schopen případně získaným klíčem dešifrovat veškerou komunikaci.

Inicializační vektor je zde 48bitový. Pro kontrolu dat je využíván MIC, který je považován za bezpečnější než CRC-32 u WEP.

WPA umožnuje dva módy autentizace – Enterprise (802.11X) a PSK (Personal). Personal používá předem sdílené klíče, které jsou poskytnuty uživatelům autorizovaným pomocí hesla. Je často využíván v domácích sítích, zatímco Enterprise, jak už z názvu vypovídá, se zaměřuje více na firemní nebo podnikové řešení, kdy je k autentizaci potřeba autentizační server.

WPA také přišlo s metodou vyjednání šifrovacích klíčů pomocí 4way handshake, tyto PTK klíče používá klient a AP k šifrování své komunikace.



Obrázek - 4-Way handshake (2)

### WPA2

Velice populární a dodnes aktuální šifrovací metoda. Kombinuje funkcionality WPA, oproti TKIP využívá CCMP, který zajišťuje integritu dat na síti a jako šifrovací algoritmus používá AES, který je dodnes dostačující.

WPA2 zajišťuje implementaci a vyhovění všech požadavků standardu 802.11i, který vylepšuje autentizaci a šifrovaní pro sítě wifi.

### WPA3

WPA3 Personal již neautentizuje pomocí PSK klíčů a nahrazuje jej pomocí PAKE a šifrovacího algoritmu SAE, který zajišťuje bezpečnou výměnu klíčů i v případě slabšího hesla. WPA3 Enterprise nabízí šifrování 256bitovými klíči, takovéto opatření přináší větší odolnost vůči útokům s moderním hardwarem a splňuje normu CNSA, která je doporučena pro vysoce citlivé aplikace.

WPA3 také přidává metodu zabezpečení komunikace na otevřených wifi sítích pomocí standardu zvaného OWE. Ten šifruje komunikaci klientů s AP napříč tomu, že nevyžaduje heslo. Každý klient používá pro šifrovanou komunikaci vlastní unikátní klíč.

Dalším novým mechanismem je DPP označovaný jako Wi-Fi Easy Connect, který je bezpečným nástupcem WPS. Byl navržen pro snazší a pohodlnější připojení zařízení bez obrazovek (typicky IoT) do wifi sítí. Namísto slabého pinu DPP využívá QR kódy nebo NFC technologii k připojení zařízení. Easy Connect byl následně také rozšířen do WPA2.

## Enterprise autentizace

Tento mechanismus je podporován pouze u WPA2/WPA3, je označován jako standard 802.11X a je dále také využíván u ethernetových sítí.

Nepoužívá PSK klíče k autentifikaci jako Personal. K ověřování využívá univerzální autentizační framework EAP, který se dále dělí. EAP-TLS ověřuje na základě certifikátů na obou stranách. Dále se potkáme s PEAP, který nevyžaduje klientský certifikát a ověřuje klienta přihlašovacími údaji z AD. Používaný je také EAP-FAST (Cisco).

### RADIUS server

RADIUS je autorizační protokol, který ověřuje uživatele a spravuje jejich přístupy na síti.

Klienty může autentifikovat pomocí certifikátů nebo uživatelských údajů. Výhodou formy ověřování certifikáty je, že je síťový administrátor nasadí na uživatelská zařízení pomocí MDM nebo group policy a uživatelé pak již nemusí dále řešit hesla k wifi. Současně to také eliminuje možnost použití slabého hesla uživatelem. Na druhou stranu ověřování pomocí uživatelských údajů je pohodlné pro nasazení do již zavedeného prostředí AD.

RADIUS server můžeme mít externí, cloudový, ale může také být zabudovaný přímo v access pointu. Je také schopný pomocí funkce „Per-User VLAN Tagging“ automaticky dle certifikátu či přihlašovacích údajů rozřazovat uživatele do různých VLAN.

## Zjednodušená autentizace ve WiFi sítích

S příchodem IoT se velice zpopularizovalo používání chytrých zařízení jako jsou IP kamery, termostaty, chytré zámky a mnoho dalšího i v běžné domácnosti. Tento okruh zařízení obohacující chod domácnosti nazýváme “chytrá domácnost”. Tyto zařízení potřebují být k možnosti komunikace a nastavení vzájemně propojení. I přesto že existují řešení pro IoT jako je ZigBee, tak stále veliká část těchto prvků využívá nejčastěji síť wifi. Pro usnadnění připojení k wifi IoT zařízení, které mají většinou omezené možnosti uživatelského rozhraní, byla vyvinuta technologie WPS. Ta se ale později prohlásila za nebezpečnou kvůli útokům využívajících slabin této technologie. S příchodem Wifi 6 bylo vyvinuto bezpečné DPP splňující dnešní standardy pro běžné použití.

### WPS (Wi-Fi Protected Setup)

Tato technologie umožňuje zařízením alternativní možnost připojení k wifi síti, a to více způsoby. Prvním je, že určitou dobu po zmáčknutí WPS tlačítka na routeru, lze připojit jakékoliv zařízení podporující wifi bez nutnosti zadání hesla. Při tomto scénáři AP klientovi pomocí navázaného spojení handshakem předává heslo k síti. Klient si heslo ukládá a má tak k dispozici přístup k síti i po uplynutí časové lhůty, kdy je WPS aktivní po stisku. Některá klientská zařízení mohou mít tlačítko WPS také, v takovémto případě se pro autentizaci spínají obě tlačítka. Druhá forma zjednodušené autentizace funguje na bázi 8číselného PINu, který funguje jako alternativa pro přihlašování heslem. Tento PIN je náhodně vygenerován při zapnutí funkce WPS na routeru a je možné ho manuálně zvolit. K autentizaci musí klient vyplnit 8číselný PIN místo hesla a router následně klienta autentifikuje právě pomocí zadaného PINu.



Obrázek - Detail WPS tlačítka (3)

### DPP (Device Provisioning Protocol)

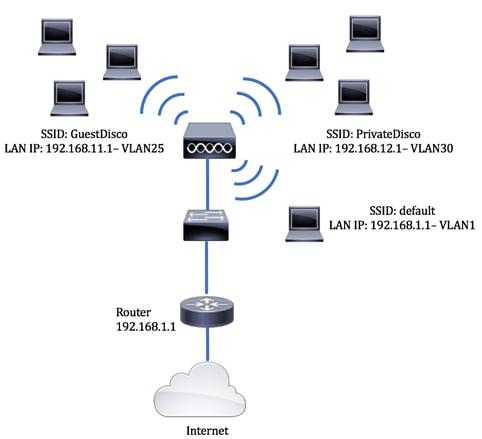
DPP neboli The Device Provisioning Protocol je technologie nahrazující zaostalé WPS. Bývá také marketingově označován jako Wifi Easy Connect. K šifrování hesla přenášeného mezi klientem a AP je využíván ECDH.

Prvky využívající DPP se rozdělují na Enrollee - klient, který se chce připojit k wifi pomocí DPP, Configurator - zařízení, které je již autentizováno a připojeno k wifi a poskytuje šifrování heslo enrollee zařízení. Poslední je Connector, to je speciální handshake, který je odpovědný za bezpečné předání.

V případě, že se enrollee chce připojit do sítě, configurator vygeneruje DPP URI sítě, která obsahuje veřejný bootstrapping klíč zařízení. Připojované zařízení má dva způsoby, jakým URI dostat – pomocí QR kódu nebo bezdrátových technologií jako je bluetooth nebo NFC. Po obdržení DPP URI naváží zařízení zabezpečené spojení pomocí ECDH. Dalo by se to nazvat privátním tunelem, ve kterém využívají své veřejné klíče k šifrování své komunikace. Přes takovýto šifrovaný tunel je následně konfigurátorem přeposíláno heslo, není ale přenášeno v plain textové podobě, ale ve formě již zmiňovaného connectoru, který umí dešifrovat pouze konkrétní zařízení.

## Segmentace sítě

Tato praktika, která se využívá nejen u wifi. Pomáhá zvyšovat bezpečnost a efektivitu správy sítě tím, že rozděluje velkou síť na menší, oddělené části nebo segmenty dle struktury filmy např.: vedení, zaměstnanci. Každý segment může mít své vlastní bezpečnostní politiky a monitoring. To umožnuje správcům efektivněji spravovat a řídit menší segmenty sítě než jednu velkou síť. Segmentaci sítě nejčastěji zajišťuje VLAN. Ta u access pointu funguje tak, že zobrazuje pro každou VLAN vlastní SSID a klientovi rámce jsou následně tagovány příslušným VLAN tagem pro danou virtuální síť. Zařízení pak mohou komunikovat pouze v rámci své virtuální sítě. Ke komunikaci mezi sítěmi VLAN je pak potřeba správně nakonfigurovaný směrovač.



Obrázek - Schéma wifi VLAN (4)

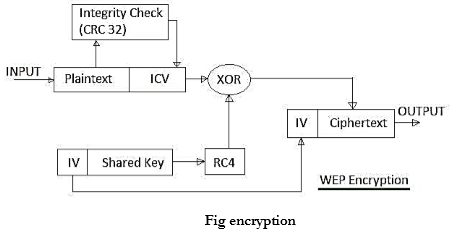
# Bezpečnostní slabiny WiFi

Bezpečnostní slabiny WiFi jsou v dnešní době velice častým cílem útoků díky hojné popularitě této technologie. Mezi nejčastější bezpečnostní rizika patří odposlouchávání či neoprávněný přístup do sítě, což jsou praktiky, proti kterým je potřeba se bránit.

## WEP

Oproti ostatním standardům má WEP hned několik slabin. První je jeho zranitelností je jeho fixní 64bitový nebo 128bitový klíč, který pro tuto dobu již považovaný za nedostatečný. I přesto, že byl v budoucnu obohacen o 256bitový klíč není tento standard považován za bezpečný. Jeho největší slabinou totiž není jeho délka klíče, ale způsob, jakým je klíč tvořen. WEP k šifrování používá statické klíče. To v praxi znamená, že každé zařízení na síti používá identický klíč. Proto je k tomuto klíči pro každý paket přidáván náhodné 24bitové číslo neboli inicializační vektor. Ten má zajistit různorodost klíče a je nešifrovaně obsáhnut v poslaném paketu, jelikož ho následně příjemce používá k dešifrování. Iniciační vektor se díky jeho nízkému počtu kombinací ve větší síti rychle začne opakovat.

Tohoto útočník dokáže snadno využít. Prvně začne tím, že zachytí velké množství paketů například pomocí nástroje wireshark. Z těchto paketů získá různé variace inicializačních vektorů, které se v síti objevují. Čím více tím větší šance, že bude klíč prolomen. Pak pomocí FMS nebo KoreK matematických algoritmů využívajících statistické vzorce je útočník schopen odvodit sdílený klíč neboli heslo k síti bez nutnosti slovníkového útoku. Tento zastaralý standard by tedy již z bezpečnostních důvodů neměl být využíván.



Obrázek - Šifrování WEP (5)

## Prolomení 4-Way handshake

Tímto typem útoku může útočník získat potřebný klíč pro dešifrovaní komunikace mezi access pointem a supplicantem neboli klientem nebo může kombinací s útokem hrubou silou získat heslo k wifi síti. Tento útok funguje na wifi sítě zabezpečené pomocí WPA nebo WPA2 autentizovaný pomocí pre-shared klíče PSK. To znamená, že náchylnými jsou šifrovací metody WPA Personal a WPA2 Personal. Doporučenou obranou proti tomuto typu útoku je nastavení silného hesla (ideálně 12místné se speciálními znaky a čísli) nebo přechod na IEEE 802.11X neboli Enterprise, který k autentizaci nepoužívá PSK, ale EAP/PEAP.

### Vyjednání šifrovacích klíčů

Průběh vyjednávání šifrovacích klíčů PTK a GTK je následující: AP i klient mají svůj PMK derivovaný z PSK a SSID. První EAPOL zpráva je poslána klientovi nazývá se Anonce. Pomocí Anonce, Snonce, PMK a MAC adres klienta a Access pointu klient odvodí svůj PTK. V druhé EAPOL zprávě posílá klient access pointu Snonce a MIC, kterým si druhá strana ověří kontrolu integrity dat. Tím je zajištěno, že data nebyla po cestě změněna. Access point obdobným způsobem odvodí svůj PTK. V případě že klient zadal špatný PSK (heslo na wifi), by access point v teto chvíli ukončil process vyjednávání klíčů a na další dva kroky by již nedošlo. V případě, že zadal klient správný PSK je poslána třetí EAPOL message klientovi se zašifrovaným GTK společně s MIC. Klíč GTK si klient ukládá a posílá čtvrtou a poslední EAPOL message oznamující access pointu, že má oba potřebné klíče a je připraven na šifrovanou komunikaci. Tento process probíhá při každé autentizaci nového zařízení do sítě.

Obsah obrázku text, snímek obrazovky, diagram, Písmo

Popis byl vytvořen automaticky

Obrázek - Vyjednání šifrovacích klíčů (6)

### Brute force na handshake

Cílem útočníka je zachytit EAPOL zprávy posílané mezi klientem a access pointem v rámci 4-Way handshake. K dosažení tohoto může buďto vyslat na access point deautentifikační paket, který vynutí konkrétnímu nebo všem klientům na síti znovu provést autentizaci nebo jednoduše vyčká na příchod nového zařízení do sítě. V případě, že zachytí handshake a získá všechny potřebné hodnoty k vygenerování PTK, může útočník zkoušet různé kombinace hesel a konstruovat pomocí nich vlastní PTK. Pokud útočníkem zkonstruovaný PTK odpovídá zachycenému PTK, heslo do sítě je prolomeno.

## WPS

První zřejmou slabinou WPS je, že každý, kdo má fyzický přístup k routeru má možnost zmáčknout WPS tlačítko a dostat se jak do sítě bez nutnosti znát jakékoliv heslo či PIN. Dále je WPS náchylné na další komplexnější útoky, které autor rozebere níže. Oproti prolomení handshake u WPA je u tohoto protokolu jedinou možností efektivní ochrany protokol kompletně vypnout a přejít na novější a bezpečnější DPP.

### Brute force

Tento útok probíhá „online” a útočník se při něm zkouší různé PIN kódy oproti routeru dokud není úspěšný. Jedná se o méně efektivní útok a díky 100 miliardám kombinacím PINu je na slabších zařízeních neproveditelný. Router může mít proti tomuto typu útoku implementovaný obranný mechanismus, který je schopen dočasně vypínat WPS po zaznamenání více neúspěšných pokusů o autentizaci.

### Pixie dust

Oproti brute force útoku na WPS se jedná o „online” útok, který je mnohonásobněji efektivnější. Využívá totiž bezpečnostního nedostatku designu autentizačního PINu WPS - 8místný kód se totiž skládá ze dvou klíčů (4místného a 3místneho) a posledním číslem je kontrolní součet. WPS používá k autentizaci tuto sekvenci:

Obsah obrázku text, snímek obrazovky, software, diagram

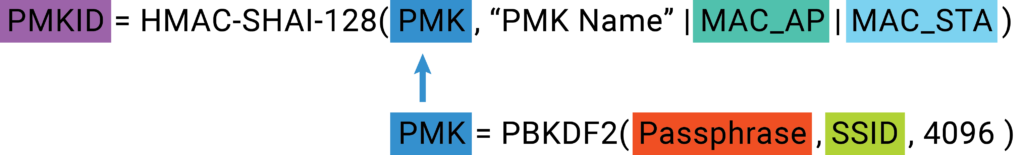
Popis byl vytvořen automaticky

Obrázek - Autentizační sekvence WPS (7)

Zachycením této sekvence získá hashované výstupy obou PINů a potřebné hodnoty k replikovaní algoritmu generujícího tyto hashované výstupy. Tímto způsobem následně útočník offline slovníkovým útokem jednotlivé klíče prolamuje každý zvlášť, což snižuje počet kombinací na 10 000 u prvního klíče a 1000 u klíče druhého. Jedná se o tak málo kombinací, že jsou tuto šifru schopni prolomit i slabší zařízení.

## PMKID

Útok na PMKID se zaměřuje na sítě využívající access point roaming definován ve standardu IEEE 802.11r. Tento mechanismus zajišťuje plynulé přepojování a přesouvaní klientů v síti z jednoho AP na druhé. Zařízení se automaticky přepojuje vždy k nejbližšímu access pointu jemu dostupnému a jeho aktivní síťové relace jsou bez přerušení přenášeny mezi AP spolu s ním. Tento standard potřebuje efektivní a rychlý způsob autentizačního procesu klienta pro plynulý přechod bez odezvy či ztráty spojení mezi access pointy. Z tohoto důvodu místo opakovaného provádění 4-Way handshake access pointy využívají funkcionalitu PMK caching, která právě pracuje s PMKID. Ten je hashem generovaným access pointem při procesu autentizace, který obsahuje PMK.



Obrázek - Detail PMKID (8)

Nebezpečnost útoku spočívá v tom, že utočník při jeho provedení nepotřebuje deautentizovat klienty jako tomu bylo u handshake prolomení, ale stačí mu jednoduše PMKID od AP vyžádat.

V případě že útočník zná SSID, MAC AP, MAC klienta a PMK, což jsou potřebné hodnoty k vygenerování PMK a následného vygenerování PMKID, může slovníkovým útokem zkoušet hesla, dokud zachycený PMKID nebude s útočníkovým vygenerovaným PMKID identický. V takové chvíli je heslo uhodnuto. Obranou proti tomuto útoku je úplné vypnutí access point roamingu v případě, že není používán či použití silného hesla wifi.

## Mann In The Middle

Skupina útoků týkajících se nejen wifi, ale mnoha dalších komunikačních technologií, kde se dává důraz na jejich bezpečnost. Primárním cílem MITM útoku je dostat odposlouchávající zařízení mezi zařízení komunikující mezi sebou aniž by o tom věděli. Výsledkem je poté únik či manipulace s daty. To může hrát klíčovou roli pro provedení dalších útoků jako je krádež identity či přihlašovacích údajů. S tímto útokem se můžeme potkat nejčastěji ve veřejných prostorech jako jsou kavárny, restaurace a bary.

### Evil Twin

Často se snaží uživatele oklamat tím, že je nakonfigurován s obdobnými parametry jako má skutečný access point například v nějaké kavárně. Často se útočník snaží nabídnout svým klientům vyšší sílu připojení, aby se jim jeho access point zobrazoval výše ve wifi nabídce než originální access point. Může se také stát, že útočník skutečný access point vyřadí rušením.



Obrázek - Evil Twin (9)

Tento typ útoku se dělí na pasivní odposlech, při kterém útočník procházející komunikaci může pouze číst a na aktivní odposlech, při kterém může útočník data upravovat a manipulovat. Zatímco pasivní odposlech útočníkovi umožní například získat citlivé údaje a hesla oběti, aktivní odposlech může vést například ke scénaři kdy útočník poslanou transakci po síti přesměruje na svůj bankovní účet.

Efektivní prevencí proti takovému útoku je opatrnost, HTTPS protokol, či využití VPN.

## Rogue AP

Jedná se o neautorizovaný access point nainstalovaný v síti bez souhlasu vlastníka. Nejčastěji se s ním potkáme ve firemních prostředích. V některých případech může být vytvořen například zaměstnancem neumýslně. I v takovémto případě se jedná o nelegalní činnost. Oproti Evil Twin je cílem otevřít backdoor do sítě a umožnit tak další útoky jako je MITM, sniffing, monitoring, phishing a další…

Obsah obrázku text, snímek obrazovky, Písmo, symbol

Popis byl vytvořen automaticky

Obrázek - Rogue AP (10)

## Wifi jamming

Tento útok využívá deautentizační rámce. To je typ management rámce, který vynutí konkrétnímu klientovi na základě MAC adresy či všem klientům na síti použítím broadcastové MAC adresy ukončit jejich spojení s access pointem. Tyto zařízení se následně do sítě dostanou opakovanou autentizací. Útok spočívá v tom, že se útočník vydává za access point (AP spoofing) a opakovaně zaplavuje síť či klienta těmito rámci. Tím docílí, že cílová zařízení opakovaně ukončují své spojení s reálným AP a tím dočasně vyřadí klienta či síť z provozu. K tomuto útoku stačí znát pouze BSSID sítě a případně MAC adresu klienta, což jsou jednoduše sniffovatelné informace. Zařízení samotná nemají žádnou možnost, jak zjistit, že se jedná o činnost útočníka nikoliv reálného AP, proto jim slepě věří. Jako prevence slouží mechanismus PMF, který nabizí pouze některé access pointy. Tento mechanismus umožňuje access pointům detekovat tyto podvržené rámce a dostatečně brzy o tom informovat své klienty. PMF je zakomponován do standardu WPA3. Na WPA3 zabezpečených sítích se tedy takového útoku není třeba bát.

# Specifikace použitých systémových komponent

V této kapitole si popíšeme systémové parametry a použitý hardware, který byl pro vývoj nástroje používán.

## Systémové specifikace

Nástroj byl vyvíjen a testován na počítači s operačním systémem Linux, konkrétně na distribuci openSUSE Tumbleweed. Zde jsou parametry a informace o platformě, získané nástrojem „neofetch“, který zobrazuje obecné informace o systému, a nástrojem „uname“, zobrazujícím verzi kernelu neboli Linuxového jádra:

Obsah obrázku text, snímek obrazovky, menu

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Informace o systému

Obsah obrázku text, snímek obrazovky, Písmo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Verze Linuxového jádra

## Bezdrátové síťové karty

Wifi karty jsou důležitou součásti pro penetrační testování wifi sítí. Tyto zařízení umožňují bezdrátovou komunikaci počítačů s přístupovými body využitím protokolu 802.11 neboli wifi.

### Tenda U10 C650

Prvním využívaným adaptérem je externí wifi adaptér Tenda U10 C650.

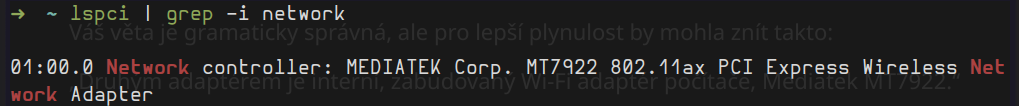
Obsah obrázku text, zeď, router, interiér

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Wifi adaptér Tenda U10

### Mediatek MT7922

Druhým adaptérem je interní, zabudovaný wifi modul počítače, Mediatek MT7922.



Obrázek - Wifi modul Mediatek MT7922

# Přístupové body

Zde si popíšeme jednotlivé přístupové body použité k připojení zařízení do testovaných wifi sítí.

## Mikrotik RB941-2nDs

První přístupový bod je Mikrotik RB941-2nD s operačním systémem RouterOS 6. Na tomto zařízení bude testováno zachycení a následné prolomení PMKID řetězce.

Obsah obrázku text, router, computer, elektronika

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Snímek Mikrotik RB941-2nDs

Obsah obrázku text, elektronika, snímek obrazovky, číslo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Systémové informace Mikrotik RB941-2nDs

## TP-Link AX23

Přístupový bod od firmy TP-Link, běžně užívaný v současných domácnostech, poslouží k testování útoků na WPA2, wifi jammingu a Evil Twin útoku.

Obsah obrázku router, interiér, elektronika, zeď

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Snímek TP-Link AX23

Obsah obrázku text, snímek obrazovky, Písmo, design

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Verze firmware TP-Link AX23

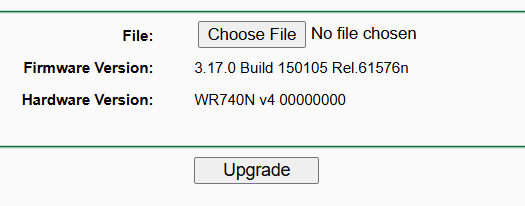
## TP-Link WR740N

Posledním využitým routerem je TP-Link starší generace, konkrétně se jedná o model WR740N. Tento router poslouží pro další testování provedených útoků na starším hardwaru.

Obsah obrázku router, interiér

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Snímek TP-Link WR740N



Obrázek - Verze firmware TP-Link WR740N

# Konfigurace vývojového prostředí

Nástroj je napsán v jazyku python kvůli jeho rozšiřitelnosti. Ke spuštění využívá virtuální prostředí pythonu, které slouží jako samostatný izolovaný prostor pro balíčky neboli knihovny nezbytné k chodu nástroje. To předchází konfliktním situacím a špatnému verzování v případě, že má uživatel více python projektů na jednom systému. Toto prostředí obsahuje potřebné doinstalované moduly neboli balíčky, rozšiřující základní python o další funkce. WiFighter také využívá určité nástroje k automatizaci útoků. Toto vše si dále popíšeme v této kapitole.

Obsah obrázku text, snímek obrazovky, diagram, Písmo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Schéma vývojového prostředí

## Využívané systémové balíčky

WiFighter využívá několik nástrojů ke svému fungování a instalaci. Tyto nástroje jsou součástí takzvaných balíčků. Tyto balíčky jsou dostupné pouze pro distribuce openSUSE a jsou instalovány pomocí správce balíčků „zypper“, který je součástí openSUSE distribucí. Na jiných Linuxových distribucích se mohou nástroje nacházet v jiných balíčcích nebo se jmenovat jinak.

Potřebné balíčky se instalují následujícím příkazem v terminálu:

Obsah obrázku text, Písmo, snímek obrazovky

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Instalace potřebných systémových balíčků

Jednotlivé balíčky si nyní představíme a popíšeme…

### Make

Nástroj make je využíván pro automatizaci kompilace a instalace potřebných nástrojů v instalačním skriptu na základě takzvané „makefile“.

### Gawk

Tento balíček obsahuje potřebný nástroj zvaný „awk“. Ten je používaný k filtraci dat z textových řetězců.

### Sed

Nástroj pro textové úpravy souborů. V instalačním skriptu je pomocí něj nastavován interpretační řádek python skriptu, specifikující, jaký interpretační program má být použít k jeho spuštění.

### Iputils

Sada nástrojů pro práci se sítěmi. Jeho součástí je potřebný nástroj „ping“, který testuje dostupnost a latenci komunikace mezi síťovými zařízeními.

### Iproute2

Sada nástrojů pro správu síťových rozhraní nahrazující balíček „net-tools“. Potřebným nástrojem z této sady je „ip“, který ulehčuje správu síťových rozhraní.

### Iw

Nástroj „iw“ umožňuje zobrazení informací a správu bezdrátových síťových rozhraní. Také je pomocí něj možné získat informace o okolních dostupných přístupových bodech.

### Python311

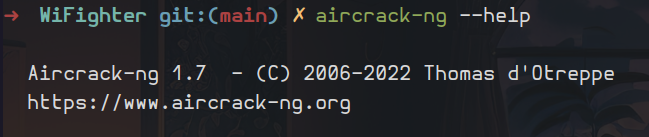
Python 3 balíček pro OpenSUSE distribuce.



Obrázek - Verze Python3

### Aircrack-ng

Sada nástrojů pro penetrační testování wifi sítí. Využívána k deautentifikaci klientů přístupového bodu, zachytávání komunikace při navazování spojení klientů s přístupovým bodem a útokům na hesla.



Obrázek - Verze Aircrack-ng

### Hashcat

Výkonný nástroj pro prolamování hashovaných řetězců. Podporuje různé hashovací algoritmy. Umožňuje hardwarovou akceleraci, rozdělení zátěže mezi grafickou kartu a procesor a paralelní zpracovaní procesů.



Obrázek - Verze Hashcat

### Pocl

Implementace OpenCL (standard pro paralelní programování), která umožňuje spuštění OpenCL programů na různých platformách. Tento balíček je potřeba pro funkčnost nástroje hashcat.

### Hostapd

Software umožňující vytvoření vlastní bezdrátové sítě na Linuxovém zařízení.

Obsah obrázku text, snímek obrazovky, Písmo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Verze Hostapd

### Dhcp-server

Tento software umožňuje nakonfigurovat a spustit vlastní server pro dynamické přidělování IP adres.

### Iptables

Nástroj pro správu firewallových pravidel zařízení.

### Coreutils

Balíček základních nástrojů potřebných pro práci s Linuxem. Na většině distribucí je tento balíček instalován již při samotné instalaci operačního systému. Obsahuje nástroje jako je například „rm“, „cd“, „tee“, „mkdir“ a mnoho dalších.

## Využívané „Hcxtools“

Hcxtools je sada nástrojů kam patří vyžadované nástroje „hcxdumptool“ verze 6.2.6 a „hcxpcapngtool“. Tyto nástroje nejsou v základu dostupné v openSUSE repozitáři balíčků. Tudíž je potřeba nainstalovat nástroje manuálně z GitHubu, což je webová platforma pro hostování a správu kódu, kde vývojáři sdílejí své projekty a spolupracují na nich. Hcxdumptool je WiFighterem využíván pro vyžádaní a zachycení PMKID řetězce od přístupového bodu, v případě, že je oběť na tento typ útoku náchylná. Hcxpcapngtool je poté následně použit pro konverzi záznamu zachycené komunikace (obsahující PMKID) do hash formátu, který je čitelný pro nástroj hashcat.

Postup instalace těchto nástrojů je následující:

Obsah obrázku text, snímek obrazovky, Písmo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Instalace Hcxtools

Instalaci nástrojů ověříme spuštěním následujících příkazů:

Obsah obrázku text, snímek obrazovky, Písmo, Grafika

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Test instalace Hcxtools

## Příprava pythonu

Prvním krokem je samostatná instalace pythonu. Distribuce openSUSE Tumbleweed již má python instalovaný v základu, ale v případě, že by tomu tak nebylo, jeho instalace byla zahrnuta v minulé kapitole příkazem „sudo zypper in -y python311“, kde „python311“ je název balíčku obsahující python3. Při vývoji byla použita následující verze:

### Virtuální prostředí

Dále je potřeba vytvořit virtuální prostředí pythonu, do kterého budou instalovány potřebné knihovny pro WiFighter.

Tímto příkazem je vytvořeno prostředí „venv“ v aktuálním adresáři:

Obsah obrázku snímek obrazovky, text, Písmo, Grafika

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Tvorba virtuálního prostředí

Následně vytvořené prostředí aktivujeme (vstoupíme do něj), což zahrnuje přesměrování cesty k Python interpretru a knihovnám, které jsou specifické pro toto virtuální prostředí.

Obsah obrázku text, snímek obrazovky, Písmo, Grafika

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Přesměrování do virtuálního prostředí

To, že se nacházíme ve virtuálním prostředí poznáme tím, že se před příkazový prompt vloží název virtuálního prostředí např.: „(venv)“. V tuto chvíli budou jakékoliv příkazy související s pythonem (python3, pip3) volány binárními soubory ve virtuálním prostředí a knihovny instalované balíčkovým správcem pythonu „pip3“ budou instalovány jen v rámci tohoto prostředí.

Nyní můžeme nainstalovat potřebné knihovny pro python.

### Scapy

Knihovna umožňující práci s pakety v pythonu. Při vývoji byla použita následující verze:

Obsah obrázku text, snímek obrazovky, Písmo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Verze knihovny Scapy

Instalace knihovny je provedena příkazem:

Obsah obrázku text, snímek obrazovky, Písmo, Grafika

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Instalace Scapy knihovny

### Prettytable

Python knihovna, která umožňuje snadné formátování a zobrazení tabulek v příkazovém řádku. Ideální pro zobrazení strukturovaných dat. Při vývoji byla použita následující verze:

Obsah obrázku text, snímek obrazovky, Písmo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Verze knihovny Prettytable

Instalace knihovny je provedena příkazem:

Obsah obrázku Písmo, text, snímek obrazovky, Grafika

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Instalace Prettytable knihovny

### Psutil

Tato knihovna umožňuje přístup k informacím o běžících procesech, jejich správu a informace o využití systémových zdrojů. Při vývoji byla použita následující verze:

Obsah obrázku text, snímek obrazovky, Písmo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Verze knihovny Psutil

Instalace knihovny je provedena příkazem:

Obsah obrázku text, Písmo, snímek obrazovky, Grafika

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Instalace Psutil knihovny

# Mechanismy nástroje a instalačního skriptu

V rámci této kapitoly si popíšeme, jak fungují jednotlivé části nástroje a instalačního skriptu.

# Instalace WiFighteru

Detailní kroky pro správnou přípravu prostředí pro nástroj, společně s instalací potřebných balíčků jsme si popsali v kapitole s názvem „Konfigurace vývojového prostředí“. Veškeré uvedené kroky automatizuje a usnadňuje instalační bash skript přiložený k nástroji, který je blíže popsán v předchozí kapitole. Tento instalační skript hraje klíčovou roli v instalaci a je nutno předem říct, že je navržen pouze pro distribuce openSUSE. Na jiných distribucích se totiž nenachází balíčkový správce „zypper“, který instalační skript využívá a balíčky můžou být jinak pojmenovány. Systém, na který je WiFighter instalován musí také disponovat zaváděcím systémem „systemd“, kterého nástroj „systemctl“ využívá WiFighter ke svému fungování. Postup instalace je také uveden na GitHub stránce nástroje.

První krokem instalace je stáhnutí repozitáře WiFighteru z GitHubu. K úspěšnému stažení musíme mít nainstalovaný balíček „git“. V případě, že tomu tak není naistalujeme tento balíček příkazem:

Obsah obrázku text, snímek obrazovky, Písmo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Instalace Git balíčku

Poté stáhneme repozitář do aktuálního adresáře následujícím příkazem:

Obsah obrázku snímek obrazovky, text, Písmo, Grafika

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Stažení WiFighter repozitáře¨

Po naklonování repozitáře se nám objeví nový adresář „WiFighter“ do kterého se přesuneme pomocí příkazu „cd“.

Obsah obrázku text, snímek obrazovky, Písmo, kruh

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Přesunutí do WiFighter adresáře

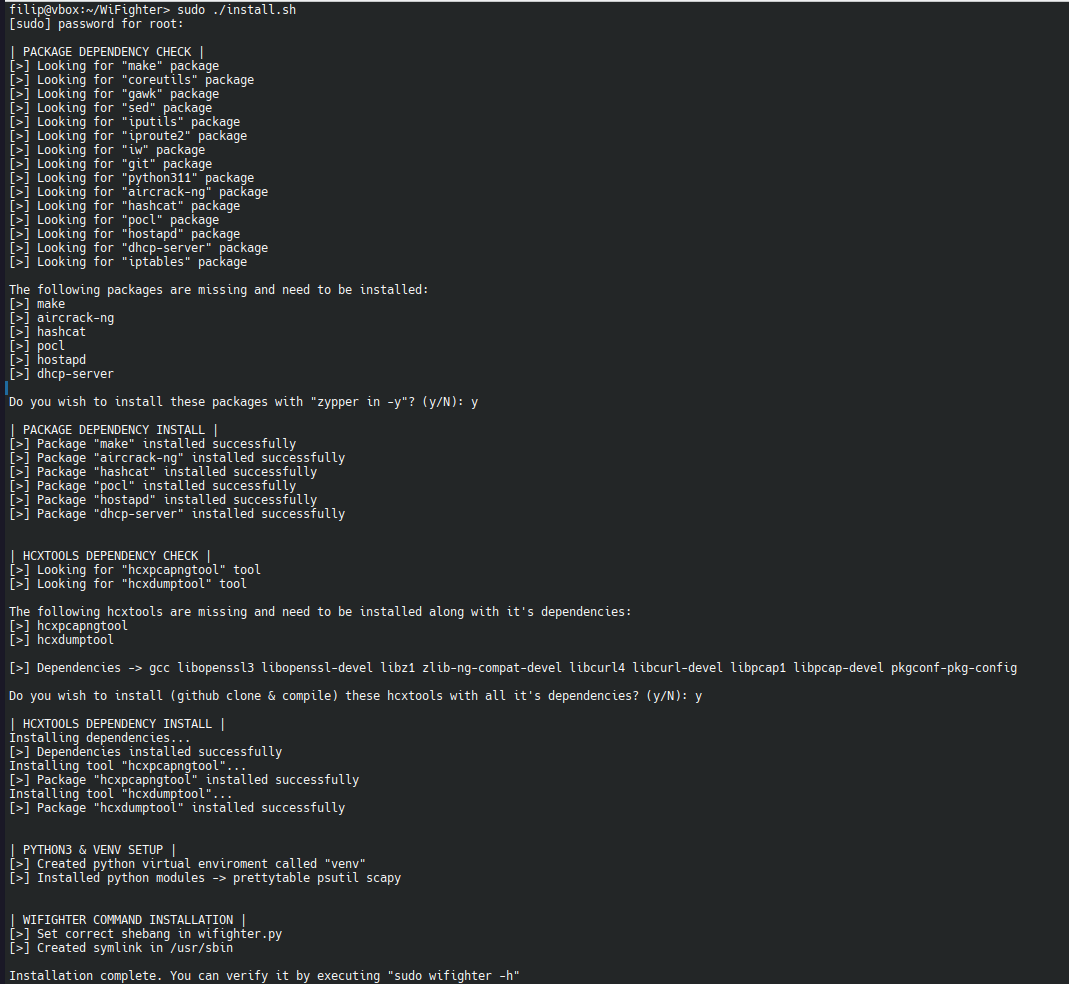
V adresáři se nachází instalační skript pro WiFighter. Přidáme mu potřebná oprávnění pro spuštění a spustíme ho pod uživatelem root. V případě, že nebude spuštěn pod uživatelem root, skript zobrazí chybovou hlášku.

Obsah obrázku text, Písmo, snímek obrazovky

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Spuštění instalačního skriptu

Skript provede kroky zmíněné v kapitole „Konfigurace vývojového prostředí“. Pokud vše proběhne v pořádku, výsledný výstup může vypadat takto:



Obrázek - Výstup úspěšného provedení instalačního skriptu

# Použití WiFighteru a jeho rozhraní

V této kapitole si projdeme jak nástroj používat, jaké jsou možnosti pro jeho používání a jak vypadá jeho rozhraní. Je nutno dodat, že nástroj (všechny příkazy s ním spojeny) je potřeba spouštět pod uživatelem root. V opačném případě vrací chybovou hlášku podobně jako tomu bylo u instalačního skriptu.

## Nápověda k nástroji

Pro zobrazení nápovědy pro použití nástroje použijeme tento příkaz:

Obsah obrázku text, snímek obrazovky

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - Nápověda k WiFighteru

## Podpříkazy nástroje

Jak je z předchozího snímku zřejmé, nástroj má několik „podpříkazů“, ty umožňují uživateli provádět akce, které by mohl v souvislosti s nástrojem potřebovat. Mezi tyto příkazy patří:

***wifighter -h, --help*** - zobrazení nápovědy

***wifighter -i, --list*** – výpis názvů dostupných bezdrátových rozhraní

***wifighter -s, --status <interface>*** - zobrazení módu (Managed/Monitor) v jakém se nachazí dané bezdrátové rozhraní

***wifighter -u, --start <interface>*** - přepnutí daného bezdrátového rozhraní do módu „Monitor“ a vypnutí služeb, které by mohli interferovat (NetworkManager, wpa\_supplicant)

***wifighter -u, --start <interface> -l, --listen <channel>*** - dodatečně k předchozímu příkazu je bezdrátové rozhraní navíc nastaveno pro poslech na specifickém kanále.

***wifighter -d, --stop <interface>*** - přepnutí daného bezdrátového rozhraní do módu „Managed“ a zapnutí služeb NetworkManager, wpa\_supplicant

***wifighter -k, --kill*** - vypnutí služeb, které by mohli interferovat (NetworkManager, wpa\_supplicant)

***wifighter -w, --wake*** - zapnutí služeb NetworkManager, wpa\_supplicant

## Rozhraní nástroje

Samotný nástroj je spouštěn příkazem „***sudo wifighter“***. Po spuštění nástroje se zobrazí výběr dostupných bezdrátových rozhraních. Vybrané rozhraní používá nástroj pro jednotlivé útoky a skenování okolních AP.

Obsah obrázku text, snímek obrazovky, Písmo, design

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - WiFighter výběr bezdrátových rozhraní

Poté se ověří zda je vybrané rozhraní v módu „Managed“ a případně je přenastaveno. Po chvíli načítaní zobrazí dostupné wifi sítě a jejich získané parametry. Tyto výsledky jsou periodicky obnovovány a případě, že chce uživatel přejít k výběru cílové wifi, musí skenování zastavit pomocí klávesové zkratky Ctrl + C a vybere cíl.

Obsah obrázku text, snímek obrazovky

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - WiFighter výsledky skenování wifi

Po výběru cílové wifi je uživatel přesměrován do výběru útoků, které má blíže popsány a také je znovu zobrazeno SSID a MAC adresa vybrané wifi.

Obsah obrázku text, snímek obrazovky, Písmo, design

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - WiFighter výběr útoků

Každý útok poté může mít své další možnosti, které jsou popsány a vybírány uživatelem.

Obsah obrázku text, snímek obrazovky, Písmo, design

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek -- WiFighter možnosti „Handshake Crack“ útoku

Obsah obrázku text, snímek obrazovky, Písmo, design

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - WiFighter možnosti "Jamming" útoku

Obsah obrázku snímek obrazovky, text

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek - WiFighter možnosti "Evil Twin" útoku

Následně je spuštěn útok dle vybraných možností a uživatel je případně dále naveden nástrojem.

ZDROJE

1. **Nextcomp.** Jak vybrat wifi router? *nextcomp.cz.* [Online] [Citace: 3. 12 2024.] https://www.nextcomp.cz/articles/105620.

2. **NetworkLessons.** WPA and WPA2 4-Way Handshake. *networklessons.com.* [Online] NetworkLessons. [Citace: 3. 12 2024.] https://networklessons.com/cisco/ccnp-encor-350-401/wpa-and-wpa2-4-way-handshake.

3. **Howdle, Dan.** Securing your Wi-Fi router: Protect your home network. *cable.co.uk.* [Online] [Citace: 3. 12 2024.] https://www.cable.co.uk/broadband/guides/router-security/.

4. **Cisco.** Configure Multiple SSIDs on a Network. *cisco.com.* [Online] Cisco. [Citace: 3. 12 2024.] https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb5652-configure-multiple-ssids-on-a-network.html.

5. **teamques10.** Explain WEP in detail. *ques10.com.* [Online] [Citace: 3. 12 2024.] https://www.ques10.com/p/14141/explain-wep-in-detail/.

6. **WiFi Professionals.** 4-Way Handshake. *wifi-professionals.com.* [Online] WiFi Professionals. [Citace: 3. 12 2024.] https://www.wifi-professionals.com/2019/01/4-way-handshake.

7. **Stepanov, Mykhailo.** [Part 2] How to Hack Into Wi-Fi – WPS Pixie Dust. *hackenproof.* [Online] [Citace: 4. listopad 2024.] https://hackenproof.com/blog/for-hackers/how-to-hack-wifi-wps-pixie-dust.

8. **Hoorvitch, Ido.** Cracking WiFi at Scale with One Simple Trick. *cyberark.* [Online] [Citace: 4. listopad 2024.] https://www.cyberark.com/resources/threat-research-blog/cracking-wifi-at-scale-with-one-simple-trick.

9. **Khan Academy.** Rogue access points. *khanacademy.org.* [Online] Khan Academy. [Citace: 3. 12 2024.] https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks.

10. **Accessagility.** Rogue Access Points. *accessagility.com .* [Online] [Citace: 3. 12 2024.] https://www.accessagility.com/rogue-wifi-wireless-access-point-ap.

11. **Vyas, Radhika.** What is WEP Security? *securew2.* [Online] [Citace: 15. říjen 2024.] https://www.securew2.com/blog/what-is-wep-security.

12. **Kinzer, Kelsey.** How Does RADIUS Improve WiFi Security? *jumpcloud.* [Online] [Citace: 16. říjen 2024.] https://jumpcloud.com/blog/radius-improve-wifi-security.

13. **Ikechukwu, Linda.** Everything You Should Know About Wi-Fi Security. *smallstep.* [Online] [Citace: 15. Říjen 2024.] https://smallstep.com/blog/everything-wifi-security/.

14. **Charlie Bromberg, Joker2a.** WPS. *thehacker.* [Online] [Citace: 4. listopad 2024.] https://www.thehacker.recipes/radio/wi-fi/wps/.

15. **Chandel, Raj.** Wireless Penetration Testing: PMKID Attack. *hackingarticles.* [Online] [Citace: 4. listopad 2024.] https://www.hackingarticles.in/wireless-penetration-testing-pmkid-attack/.

16. **Gillis, Alexander S.** Wi-Fi Protected Access (WPA). *techtarget.* [Online] [Citace: 15. říjen 2024.] https://www.techtarget.com/searchmobilecomputing/definition/Wi-Fi-Protected-Access.

17. **Gargan, Richard.** Network Access With DPP (Device Provisioning Protocol). *netmaker.* [Online] [Citace: 16. říjen 2024.] https://www.netmaker.io/resources/device-provisioning-protocol-dpp.

18. **Garakh, Iliya.** WPS – What is it, and how does it work? *passwork.* [Online] [Citace: 16. říjen 2024.] https://passwork.pro/blog/what-is-wps/.

19. **Bouška, Petr.** Cisco WiFi - základní principy a protokoly. *samuraj-cz.* [Online] [Citace: 14. Říjen 2024.] https://www.samuraj-cz.com/clanek/cisco-wifi-zakladni-principy-a-protokoly/.

20. **Cybersecura.** WPA/WPA2 cracking, PMKID, Evil Twin... Overview of attacks and threats to Wi-Fi in 2022. *cybersecura.* [Online] Cybersecura. [Citace: 3. listopad 2024.] https://www.cybersecura.com/en/post/overview-of-attacks-and-threats-to-wifi-in-2022.

21. **Ebbecke, Philipp.** Protected Management Frames enhance Wi-Fi® network security. *wi-fi.org.* [Online] [Citace: 13. 1 2025.] https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security.

22. **NetworkLessons.** Introduction to WPA Key Hierarchy. *networklessons.com.* [Online] NetworkLessons. [Citace: 11. 1 2025.] https://networklessons.com/cisco/ccnp-encor-350-401/introduction-to-wpa-key-hierarchy.

23. **NordVPN.** WEP crack. *nordvpn.com.* [Online] NordVPN. [Citace: 12. 1 2025.] https://nordvpn.com/cybersecurity/glossary/wep-crack/.

24. **Kerslager, Milan.** Prolomení WEP. *pslib.cz.* [Online] [Citace: 12. 1 2025.] https://www.pslib.cz/milan.kerslager/Prolomen%C3%AD\_WEP.

25. **ayusharma0698.** Wifi Protected Access (WPA). *geeksforgeeks.* [Online] [Citace: 14. říjen 2024.] https://www.geeksforgeeks.org/wifi-protected-access-wpa/.

26. **PODA.** Jak funguje domácí Wi-Fi. *https://www.poda.cz/.* [Online] PODA. [Citace: 14. Říjen 2024.] https://www.poda.cz/novinky/jak-funguje-domaci-wi-fi/.

27. **ZIMPERIUM.** Rogue Access Point. *https://www.zimperium.com/.* [Online] ZIMPERIUM. [Citace: 11. 1 2025.] https://www.zimperium.com/glossary/rogue-access-point/.

SEZNAM OBRÁZKŮ

[Obrázek 1 - Wifi standardy 10](#_Toc191228637)

[Obrázek 2 - 4-Way handshake 12](#_Toc191228638)

[Obrázek 3 - Detail WPS tlačítka 15](#_Toc191228639)

[Obrázek 4 - Schéma wifi VLAN 16](#_Toc191228640)

[Obrázek 5 - Šifrování WEP 17](#_Toc191228641)

[Obrázek 6 - Vyjednání šifrovacích klíčů 19](#_Toc191228642)

[Obrázek 7 - Autentizační sekvence WPS 20](#_Toc191228643)

[Obrázek 8 - Detail PMKID 21](#_Toc191228644)

[Obrázek 9 - Evil Twin 22](#_Toc191228645)

[Obrázek 10 - Rogue AP 23](#_Toc191228646)

[Obrázek 11 - Informace o systému 24](#_Toc191228647)

[Obrázek 12 - Verze Linuxového jádra 24](#_Toc191228648)

[Obrázek 13 - Wifi adaptér Tenda U10 25](#_Toc191228649)

[Obrázek 14 - Wifi modul Mediatek MT7922 25](#_Toc191228650)

[Obrázek 15 - Snímek Mikrotik RB941-2nDs 26](#_Toc191228651)

[Obrázek 16 - Systémové informace Mikrotik RB941-2nDs 26](#_Toc191228652)

[Obrázek 17 - Snímek TP-Link AX23 27](#_Toc191228653)

[Obrázek 18 - Verze firmware TP-Link AX23 27](#_Toc191228654)

[Obrázek 19 - Snímek TP-Link WR740N 28](#_Toc191228655)

[Obrázek 20 - Verze firmware TP-Link WR740N 28](#_Toc191228656)

[Obrázek 21 - Schéma vývojového prostředí 29](#_Toc191228657)

[Obrázek 22 - Instalace potřebných systémových balíčků 30](#_Toc191228658)

[Obrázek 23 - Verze Python3 31](#_Toc191228659)

[Obrázek 24 - Verze Aircrack-ng 31](#_Toc191228660)

[Obrázek 25 - Verze Hashcat 31](#_Toc191228661)

[Obrázek 26 - Verze Hostapd 32](#_Toc191228662)

[Obrázek 27 - Instalace Hcxtools 33](#_Toc191228663)

[Obrázek 28 - Test instalace Hcxtools 33](#_Toc191228664)

[Obrázek 29 - Tvorba virtuálního prostředí 34](#_Toc191228665)

[Obrázek 30 - Přesměrování do virtuálního prostředí 34](#_Toc191228666)

[Obrázek 31 - Verze knihovny Scapy 35](#_Toc191228667)

[Obrázek 32 - Instalace Scapy knihovny 35](#_Toc191228668)

[Obrázek 33 - Verze knihovny Prettytable 35](#_Toc191228669)

[Obrázek 34 - Instalace Prettytable knihovny 35](#_Toc191228670)

[Obrázek 35 - Verze knihovny Psutil 36](#_Toc191228671)

[Obrázek 36 - Instalace Psutil knihovny 36](#_Toc191228672)

[Obrázek 37 - Instalace Git balíčku 37](#_Toc191228673)

[Obrázek 38 - Stažení WiFighter repozitáře¨ 37](#_Toc191228674)

[Obrázek 39 - Přesunutí do WiFighter adresáře 37](#_Toc191228675)

[Obrázek 40 - Spuštění instalačního skriptu 38](#_Toc191228676)

[Obrázek 41 - Výstup úspěšného provedení instalačního skriptu 38](#_Toc191228677)

[Obrázek 42 - Nápověda k WiFighteru 39](#_Toc191228678)

[Obrázek 43 - WiFighter výběr bezdrátových rozhraní 40](#_Toc191228679)

[Obrázek 44 - WiFighter výsledky skenování wifi 41](#_Toc191228680)

[Obrázek 45 - WiFighter výběr útoků 41](#_Toc191228681)

[Obrázek 46 -- WiFighter možnosti „Handshake Crack“ útoku 42](#_Toc191228682)

[Obrázek 47 - WiFighter možnosti "Jamming" útoku 42](#_Toc191228683)

[Obrázek 48 - WiFighter možnosti "Evil Twin" útoku 42](#_Toc191228684)

SEZNAM ZKRATEK

WiFi, wifi, wi-fi – populární bezdrátová komunikační technologie

IEEE 802.11 – sada standardů pro wifi

AP – přístupový bod pomocí kterého se mohou zařízení připojit do wifi sítě

WEP – zastaralý bezpečnostní algoritmus wifi

WPA – již nepoužívaný bezpečnostní algoritmus wifi

WPA2 – bezpečnostní algoritmus wifi

WPA3 – nejnovější bezpečnostní algoritmus wifi

CRC-32 – hashovací algoritmus používaný pro kontrolu integrity dat

RC4 – kryptografický algoritmus používaný pro WEP

TKIP – kryptografický algoritmus používaný pro WPA

MIC – hashovací algoritmus používaný pro kontrolu integrity dat

PSK – předsdílený klíč používaný v WPA 4way handshake

PTK – klíč používaný zařízeními na WPA wifi sítích k šifrování komunikace

GTK – klíč šifrující multicast a broadcast komunikaci na WPA wifi sítích

PMK – klíč generovaný z PTK, je používán k následnému odvození PTK

CCMP – kryptografický algoritmus používaný pro WPA2

AES – standardizovaný algoritmus pro symetrické šifrování dat

PAKE – metoda bezpečného vyjednání šifrované komunikace pro WPA3

SAE – nahrazuje autentizaci předsdíleným klíčem, je používán u WPA3

CNSA – sada kryptografických algoritmů standardizovaných Národním bezpečnostní úřadem

OWE – metoda zabezpečení a šifrovaní komunikace na otevřených sítích, zahrnuta ve WPA3

DPP – bezpečná a moderní metoda přidávání zařízení do sítě bez nutnosti hesla

WPS – zastaralá metoda přidávání zařízení do sítě bez nutnosti hesla

IoT – síť propojených zařízení komunikujících přes internet, často kamery nebo senzory

NFC – bezdrátová technologie umožňující rychlý přenos dat na velmi krátké vzdálenosti

AD – adresářová databáze pro ověřovaní uživatelů a jejich oprávnění v doméně

MDM – služba pro správu mobilních koncových zařízení

VLAN – technologie umožňující rozdělení fyzické sítě na více virtuálních podsítí

PIN – osobní identifikační číslo používané k autentizaci

ECDH – varianta protokolu Diffie Hellman pro výměnu klíčů

URI – textový řetězec s definovanou strukturou využívaný převážně v internetu

SSID – identifikační název wifi sítě

BSSID – fyzická adresa přístupového bodu

EAPOL – standardizovaný sítový autentizační protokol

MAC – unikátní identifikátor síťového adaptéru zařízení

PMKID – identifikátor využívaný wifi sítěmi s povolenou funkcí fast roaming

MITM – typ útoku, ve kterém útočník poslouchá či manipuluje s daty mezi dvěma zařízeními

HTTPS – šifrovaná komunikace určená pro zobrazování webových stránek

VPN – technologie umožňující vytvoření šifrovaného tunelu mezi dvěma sítěmi

**Obrazky zdroje plain**

<https://www.nextcomp.cz/articles/105620>

<https://networklessons.com/cisco/ccnp-encor-350-401/wpa-and-wpa2-4-way-handshake>

<https://www.cable.co.uk/broadband/guides/router-security/>

<https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb5652-configure-multiple-ssids-on-a-network.html>

<https://www.ques10.com/p/14141/explain-wep-in-detail/>

<https://www.wifi-professionals.com/2019/01/4-way-handshake>

<https://hackenproof.com/blog/for-hackers/how-to-hack-wifi-wps-pixie-dust>

<https://www.cyberark.com/resources/threat-research-blog/cracking-wifi-at-scale-with-one-simple-trick>

<https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks>

<https://www.accessagility.com/rogue-wifi-wireless-access-point-ap>