Vysoká škola polytechnická Jihlava

Aplikovaná informatika

**Demonstrační nástroj Man-in-the-middle útoků na Wi-Fi sítě**

Bakalářská práce

Autor práce: Jiří Karmasin

Vedoucí práce: Mgr. Antonín Přibyl

Jihlava 2023

**Vysoká škola polytechnická Jihlava**

Tolstého 16, 586 01 Jihlava

**ZADÁNÍ BAKALÁŘSKÉ PRÁCE**

Autor práce: **Jiří Karmasin**

Studijní program: Aplikovaná informatika

Obor: Aplikovaná informatika

Název práce: **Demonstrační nástroj Man-in-the-middle útoků na Wi-Fi sítě**

Cíl práce: Cílem práce je navrhnout a implementovat demonstrační nástroj k popisu a vysvětlení principu Man-in-the-middle (MITM) útoků na bezdrátové sítě. Tento nástroj poslouží k názorným ukázkám během školení kybernetické bezpečnosti především pro příslušníky Armády České republiky, proto musí být uživatelské rozhraní dostatečně intuitivní a přehledné. Součástí nástroje bude i popis relevantních protiopatření, které zvyšují imunitu proti MITM útokům. Nástroj bude implementován na platformě KALI Linux. Rovněž budou vytvořeny návodné a dokumentační nástroje (poster, brožura) pro cílové publikum pro zvýšení účinku školení s využitím tohoto nástroje.

Abstrakt

Vlastní text.

Klíčová slova

První klíčové slovo; druhé klíčové slovo; třetí klíčové slovo

Abstract

Vlastní text.

Keywords

První klíčové slovo; druhé klíčové slovo; třetí klíčové slovo

Prohlašuji, že předložená Zvolte položku. práce je původní a zpracoval/a jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil/a autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v platném znění, dále též „**AZ**“).

Byl/a jsem seznámen/a s tím, že na mou Zvolte položku. práci se plně vztahuje **AZ**, zejména § 60 (školní dílo).

Podle § 47b zákona o vysokých školách souhlasím se zveřejněním své práce podle směrnice prorektora pro studium č. 2/2020, a to bez ohledu na výsledek obhajoby.

Beru na vědomí, že VŠPJ má právo na uzavření licenční smlouvy o užití mé Zvolte položku. práce a prohlašuji, že **souhlasím** s případným užitím mé Zvolte položku. práce (prodej, zapůjčení apod.).

Jsem si vědom/a toho, že užít své Zvolte položku. práce či poskytnout licenci k jejímu využití mohu jen se souhlasem VŠPJ, která má právo ode mě požadovat přiměřený příspěvek na úhradu nákladů, vynaložených vysokou školou na vytvoření díla (až do jejich skutečné výše), z výdělku dosaženého v souvislosti s užitím díla či poskytnutím licence.

V Jihlavě dne Klikněte nebo klepněte sem a zadejte datum.

…………………………………….

Podpis studenta

Poděkování

*Na tomto místě můžete poděkovat všem, kteří si to podle vašeho úsudku zaslouží (např. vedoucí práce, konzultant, rodina atd.)*

*Vlastní text poděkování.*

Obsah

[Seznam obrázků 7](#_Toc151746691)

[Seznam tabulek 8](#_Toc151746692)

[Seznam zkratek 9](#_Toc151746693)

[Úvod 10](#_Toc151746694)

[1 Analýza síťových protokolů 11](#_Toc151746695)

[1.1 OSI model 11](#_Toc151746696)

[1.2 ARP 11](#_Toc151746697)

[1.3 Handshake 12](#_Toc151746698)

[1.4 WEP 12](#_Toc151746699)

[1.5 WPA, WPA2 12](#_Toc151746700)

[1.6 WPS 12](#_Toc151746701)

[1.7 SSL 12](#_Toc151746702)

[2 Analýza vektorů útoku 13](#_Toc151746703)

[2.1 Aplikace MITM 13](#_Toc151746704)

[2.2 ARP poisoning + (MAC flooding) 13](#_Toc151746705)

[2.3 SSLsplit 13](#_Toc151746706)

[2.4 Analýza existujících nástrojů 13](#_Toc151746707)

[3 Návrh implementace 14](#_Toc151746708)

[3.1 Zdůvodnění použitého jazyka implementace 14](#_Toc151746709)

[3.2 Návrh funkcionalit konzolového back-endu 14](#_Toc151746710)

[3.3 Návrh GUI 14](#_Toc151746711)

[4 Implementace 15](#_Toc151746712)

[4.1 Implementace konzolového back-endu 15](#_Toc151746713)

[4.2 Implementace GUI 15](#_Toc151746714)

[5 Testování 16](#_Toc151746715)

[5.1 Testy funkčnosti 16](#_Toc151746716)

[5.2 Testy výkonosti 16](#_Toc151746717)

[Závěr 17](#_Toc151746718)

[Seznam použité literatury 18](#_Toc151746719)

[Přílohy 19](#_Toc151746720)

# Seznam obrázků

# Seznam tabulek

# Seznam zkratek

AČR Armáda České republiky

NATO North Atlantic Treaty Organization (Severoatlantická aliance)

NÚKIB Nádorní úřad pro kybernetickou a informační bezpečnost

MITM Man-in-the-middle

MAC Medium Access Control

IP Internet protocol

TCP Transmission Control Protocol

UDP User datagram protocol

EAPOL Extensible authentication protocol over LAN

LAN Local area network

# Úvod

Dnešní svět se stále více digitalizovaný. To s sebou nese mnoho pozitivních jevů jako je zvýšení produktivity téměř všech lidských činností, rychlost komunikace mezi lidmi a možnost mít všechny myslitelné informace doslova na dlani kdykoliv si člověk přeje. Mimoto však s sebou přináší i mnoho bezpečnostních hrozeb a zranitelností, které před příchodem digitálního věku neexistovaly.

Kybernetická bezpečnost se tedy stává jedním z nejnaléhavějších problémů, kterým čelíme v této době. Jedním z hlavních způsobů, kterým zvyšovat bezpečnost v kyberprostoru, je dle vyjádření NÚKIB školení a osvěta v oblasti kybernetické bezpečnosti a chování v digitálním prostoru. Školení jsou klíčová pro posilování odolnosti organizací vůči kybernetickým útokům.

Jako specialista kybernetické bezpečnosti sloužící v Armádě České republiky je mojí povinností takováto školení provádět. Z mých letitých zkušeností je zřejmé, že teoretický výklad na povinných školeních nemá zdaleka takový dopad jako praktická ukázka probírané látky. A právě proto se moje bakalářská práce zaměřuje na návrh a implementaci demonstračního nástroje, který má za cíl poskytnout názorné ukázky útoku man-in-the-middle (MITM) a tím pomoci školitelům a studentům lépe porozumět této kybernetické hrozbě.

MITM útoky patří mezi nebezpečné techniky, při kterých útočník vstupuje mezi komunikující strany a může odposlouchávat a modifikovat datový tok. Tato zranitelnost Wi-Fi sítí je známá a často zneužívaná, což pro příslušníky resortu Ministerstva obrany představuje hrozbu při využívání Wi-Fi připojení k internetu.

Cílovým publikem bude široká škála posluchačů při školení od neznalých uživatelů koncových zařízení (smartphonů) až po IT techniky a síťové administrátory. Každému posluchači by při tom měla demonstrační ukázka přinést nový poznatek. Výsledný nástroj by tedy měl být přehledný, a přitom měl mít možnost poskytovat hlubší a komplexnější informace o fázích útoku, pokud by to o měl posluchač zájem.

Práce bude dále diskutovat o klíčových aspektech man-in-the-middle útoků, jejich důsledcích, a především ochranných opatřeních proti nim. Kromě toho popíše proces vývoje demonstračního nástroje.

Cílem práce je tedy nejen vytvořit funkční nástroj pro demonstrace, ale také přispět k zvýšení povědomí o MITM útocích a zlepšení schopností obrany proti nim. Věříme, že vypracovaný projekt má potenciál přispět k bezpečnosti digitálního prostoru a k lepší přípravě jednotlivců na výzvy, které s sebou nese kybernetická éra.

# Analýza síťových protokolů

Bezdrátovou komunikaci, jejíž napadení bude práce demonstrovat je Wi-Fi. Wi-Fi připojení koncových zařízení k internetu využívá sadu standardizovaných protokolů IEEE 802, díky kterým je vůbec možné samotnou komunikaci navázat a provozovat. V první části práce popíšu a analyzuji základní sadu protokolů. Na tuto analýzu budu navazovat v následující části práce, kde se zaměřím na slabá místa jednotlivých částí komunikace. Dobře znát princip těchto protokolů je tedy zásadní pro pozdější zneužití jejich zranitelností.

## OSI model

Obsah obrázku text, snímek obrazovky, Písmo

Popis byl vytvořen automaticky

*Zdroj: wikipedia.org*

Útok MITM probíhá na 2. spojové (neboli linkové) vrstvě referenčního ISO/OSI modelu

## ARP

ARP je zkratka „adress resolution protocol“. Jeho účelem je převod fyzické MAC adresy na síťovou IP adresu. Aby mohlo zařízení připojené do sítě komunikovat s okolními zařízeními v bezprostřední blízkosti, musí TODO

ARP request

ARP response

## Handshake

## WEP

*Podrobnější informace naleznete v článku* [*Wired Equivalent Privacy*](https://cs.wikipedia.org/wiki/Wired_Equivalent_Privacy)*.*

[*Šifrování*](https://cs.wikipedia.org/wiki/Kryptografie) *komunikace pomocí statických* [*WEP*](https://cs.wikipedia.org/wiki/Wired_Equivalent_Privacy) *klíčů (Wired Equivalent Privacy)* [*symetrické šifry*](https://cs.wikipedia.org/wiki/Symetrick%C3%A1_kryptografie)*, které jsou ručně nastaveny na obou stranách bezdrátového spojení. Kvůli nedostatkům v protokolu lze zachycením specifických rámců a jejich analýzou lze klíč relativně snadno získat (programem* [*Aircrack-ng*](https://cs.wikipedia.org/wiki/Aircrack-ng)*). Autentizace přístupu do WPA sítě je prováděno pomocí PSK ([Pre-shared key](https://cs.wikipedia.org/wiki/Pre-shared_key" \o "Pre-shared key) – obě strany používají stejnou dostatečně dlouhou* [*heslovou frázi*](https://cs.wikipedia.org/wiki/Heslo)*),* [*RADIUS*](https://cs.wikipedia.org/wiki/RADIUS) *serverem (ověřování přihlašovacím jménem a heslem) nebo dalšími variantami* [*EAP*](https://cs.wikipedia.org/wiki/Extensible_Authentication_Protocol) *protokolu.*

## WPA, WPA2

*Podrobnější informace naleznete v článku* [*Wi-Fi Protected Access*](https://cs.wikipedia.org/wiki/Wi-Fi_Protected_Access)*.*

*Kvůli zpětné kompatibilitě využívá* [*WPA*](https://cs.wikipedia.org/wiki/Wi-Fi_Protected_Access) *(Wi-Fi Protected Access) WEP klíče, které jsou ale často dynamicky bezpečným způsobem měněny (protokoly TKIP, CCMP). Pro průběžnou změnu klíčů slouží speciální doprovodný program, který nazýváme prosebník (suplikant). Z tohoto důvodu bylo možné doplnit WPA i do staršího hardware a výrobci nemuseli uvádět na trh úplně nová zařízení. PSK klíč lze zjistit pouze slovníkovou metodou (tj. zkoušením různých hesel proti odposlechnuté variantě úspěšné autentizace).*

*Podrobnější informace naleznete v článku* [*IEEE 802.11i*](https://cs.wikipedia.org/wiki/IEEE_802.11i)*.*

*Novější* [*WPA2*](https://cs.wikipedia.org/wiki/IEEE_802.11i) *přináší kvalitnější šifrování (šifra AES), která však vyžaduje větší výpočetní výkon, a proto nelze WPA2 používat na starších zařízeních.*

## WPS

*Podrobnější informace naleznete v článku* [*Wi-Fi Protected Setup*](https://cs.wikipedia.org/wiki/Wi-Fi_Protected_Setup)*.*

*Pro snadnější připojení do bezdrátové sítě je možné se připojit pomocí* [*WPS*](https://cs.wikipedia.org/wiki/Wi-Fi_Protected_Setup)*. Na zařízení může být WPS tlačítko, kdy po jeho zmáčknutí lze se po omezený čas do bezdrátové sítě připojit bez autentizace. Místo tlačítka může být zadán osmimístný PIN (oba způsoby lze kombinovat). Číselný kód však lze v poměrně krátké době uhádnout zkoušením různých variant. Novější zařízení proto obsahují omezení počtu pokusů o připojení, případně lze WPS úplně vypnout.*

## SSL

# Analýza vektorů útoku

15

Základní charakteristikou, která odlišuje bezdrátové připojení od Ethernetového je všesměrové elektromagnetické vysílání komunikujících stran. Tyto rámce tedy mohou být zachyceny a zpracovány kýmkoliv v dosahu signálu.

## Aplikace MITM

### Lámání WEP2 hesla

## ARP poisoning + (MAC flooding)

## SSLsplit

## Analýza existujících nástrojů

# Návrh implementace

27

## Zdůvodnění použitého jazyka implementace

## Návrh funkcionalit konzolového back-endu

## Návrh GUI

# Implementace

## Implementace konzolového back-endu

### EvilTwin Wi-Fi

### ARPspoof

## Implementace GUI

# Testování

## Testy funkčnosti

## Testy výkonosti

# Závěr

# Seznam použité literatury

<https://cs.wikipedia.org/wiki/Wi-Fi>

<file:///D:/1_HACK/CYBER%20BOOKS/ethical_hacking_and_penetration_testing_guide.pdf>

<https://prabhjeetlearning.medium.com/capturing-a-wi-fi-handshake-the-key-to-network-security-testing-d7aad39b3fdf>

# Přílohy