

**PROJEKT Č. 3**

**Penetrační testování sondy SonIoT**

B0B32KTI - Komunikační technologie pro IoT

Jan Tonner, Petr Procházka, Petr Kučera

28. 10. 2022 | ČVUT Praha

# Obsah

[**Abstrakt**](#_e3arxjr4tpx9) **4**

[Cíl projektu](#_ffyidc1i3avt) 4

[Stručný závěr projektu](#_21ommofpuhq) 4

[**Průběh projektu**](#_ye6trn6zmyzu) **5**

[Zadání projektu](#_cerdhsfr4mjw) 5

[Naplánování spolupráce](#_ihtt9dvsprcn) 5

[Průběh práce](#_fwj3b5xbwrpq) 6

[Rešerše](#_neh9eca8r9o) 6

[Penetrační testování](#_dgpdtq2y4xp1) 6

[Typy testů](#_ul8sex4lgyg5) 6

[Dle postavení útočníka](#_gyvztt265707) 6

[Dle znalosti systému](#_kta0l171iyfq) 6

[Dle typů provedení](#_mnr2k0u9br50) 6

[Analýza testované infrastruktury](#_1fe0o9i66mkm) 6

[Měření](#_u6cwt57hhytd) 8

[1. Zjištění služeb, které používá sonda](#_z024o35afucg) 8

[Snippet kódu](#_aowmk5fpdbqp) 8

[Screenshot](#_w6l6yga6zzj0) 8

[Hodnocení úspěšnosti](#_l7eeelbrwn0t) 8

[Vytížení sondy](#_fdxwqjjs642g) 8

[2. Slovníkový útok na login pomocí Metasploit](#_fbkr9gar8y3c) 9

[Screenshot](#_608ywifz6fi0) 9

[Hodnocení úspěšnosti](#_if7ewhhsj8sb) 9

[Vytížení sondy](#_k7zrswtedcg5) 9

[3. Brute Force na SSH pomocí hydry](#_7sqn7qcaoga7) 10

[Snippet kódu](#_xpksi2jbdkvy) 10

[Screenshot](#_os868btuavk1) 10

[Hodnocení úspěšnosti](#_bm6fs3o5oagb) 10

[Vytížení sondy](#_w75idz4cnn6t) 10

[4. Mapování zařízení v síti pomocí](#_gckejny9f9as) 11

[Snippet kódu](#_55103w4w4mjl) 11

[Screenshot](#_kb9joj3zsrc4) 11

[Hodnocení úspěšnosti](#_3zud3639s5nm) 11

[Vytížení sondy](#_ikux7erzct57) 11

[5. Monkey HTTPD Header Parsing Denial of Service (DoS)](#_l83atrh1efp) 12

[Popis scénáře](#_ch8dg9cty9pb) 12

[Screenshot](#_ov7ecsur7c7c) 12

[Hodnocení úspěšnosti](#_9ocxunsa9w1q) 12

[Vytížení sondy](#_gpml3ev10l0y) 12

[6. Mapovani portu na koncentratoru](#_1v7bdyrojm8g) 13

[Snippet kódu](#_lrzxpm2shrr6) 13

[Screenshot](#_3meghfift49v) 13

[Hodnocení úspěšnosti](#_utjqtkkbdmhp) 13

[Vytížení sondy](#_q3peg04n1sze) 13

[Závěr práce](#_35zbqaokwqq) 13

[Zhodnocení měření](#_f7nojchrb7e2) 14

[Zhodnocení spolupráce](#_nd9vvo5axb0o) 14

[**Zdroje**](#_yazzxhksboyh) **14**

[Literatura a reference](#_iqwscoldhmy) 15

# Abstrakt

## Cíl projektu

Cílem třetího projektu je nastudovat možnosti penetračního testování skrze telekomunikační síť a ze získaných informací sestavit sadu testů, respektive útoků namířených na sondu. V závěru diskutovat úspěšnost.

## Stručný závěr projektu

Během projektu jsme se naučili pracovat s základními bezpečnostními funkcemi, seznámili se s podstatou penetračního testování.

Měření na sondě dopadlo podle očekávání. Sondě se povedlo úspěšně rozlišit závažnost útoků.

# 

# Průběh projektu

## Zadání projektu

Studenti si nastudují možnosti penetračního testování koncových zařízení skrze telekomunikační síť, např. článek[[1]](#footnote-0) či článek[[2]](#footnote-1) a další. Z rešerše vytvořené na základě nastudovaných poznatků si připraví sadu testů, resp. útoků a ty v rámci předem předpřipravené infrastruktury aplikují na sondu a to v libovolné variantě, tj. IDS nebo IPS. Studenti zároveň kontrolují logy z nástroje Suricata a identifikují ty, které značí zachycený test/útok.

Pro různé druhy útoků je požadováno zaznamenání těchto parametrů:

* typ útoku,
* zdroj a cíl útoku,
* byl útok zaznamenán? ANO/NE (v případě nejasného výsledku slovní zhodnocení),
* hardwarové využití sondy na typy útoků.

Studenti následně slovně zhodnotí a číselně vyhodnotí efektivnost detekce.

## Naplánování spolupráce

Na tomto projektu budeme spolupracovat online, z důvodu ušetření času. Jelikož nikdo z nás nemá s bezpečnostním testováním žádné zkušenosti, každý si nejprve prostudujeme problematiku a připravíme několik konkrétních scénářů. Poté si zavoláme, předáme, co kdo zjistil a sestavíme konkrétní sadu testů, které společně vyhodnotíme. V závěru budeme vše diskutovat.

## Průběh práce

### Rešerše

#### Penetrační testování

**Penetrační testování** je disciplína, která si klade za cíl otestovat bezpečnost informačních systémů pomocí simulovaných útoků a podat souhrnou zprávu o stavu systému.

K takovému typu testování je vhodné využívat **specializovaných** **nástrojů**, které jsou určené přímo pro penetrační testování. Mezi oblíbené verze operačních systémů patří např. [Kali Linux](https://www.kali.org/) nebo [BlackArch](https://blackarch.org/) a mezi softwarové balíčky s již předpřipravenými testy např. [Metasploit](https://www.metasploit.com/) či [w3af](http://w3af.org/).[[3]](#footnote-2)

#### Typy testů

##### Dle postavení útočníka

**Externí testy** jsou prováděny z vnější strany testované sítě např. útok hackera z internetu.

**Interní testy** jsou prováděny z vnitřní strany dané sítě. Snaží se simulovat situaci, v které by měl útočník přístup do interní sítě či se jednalo o neloajální zaměstnance.

##### Dle znalosti systému

**Black-box test** - simulována situace, kdy neznám infrastrukturu dané sítě či aplikace.

**Grey-box test** - útočník má poze elementární znalost systému.

**White-box test** - útočník má celkovou znalost o systému. Zná topologii, rozumí jednotlivým prvkům.

##### Dle typů provedení

**Manuální testy** - testy specificky na míru.

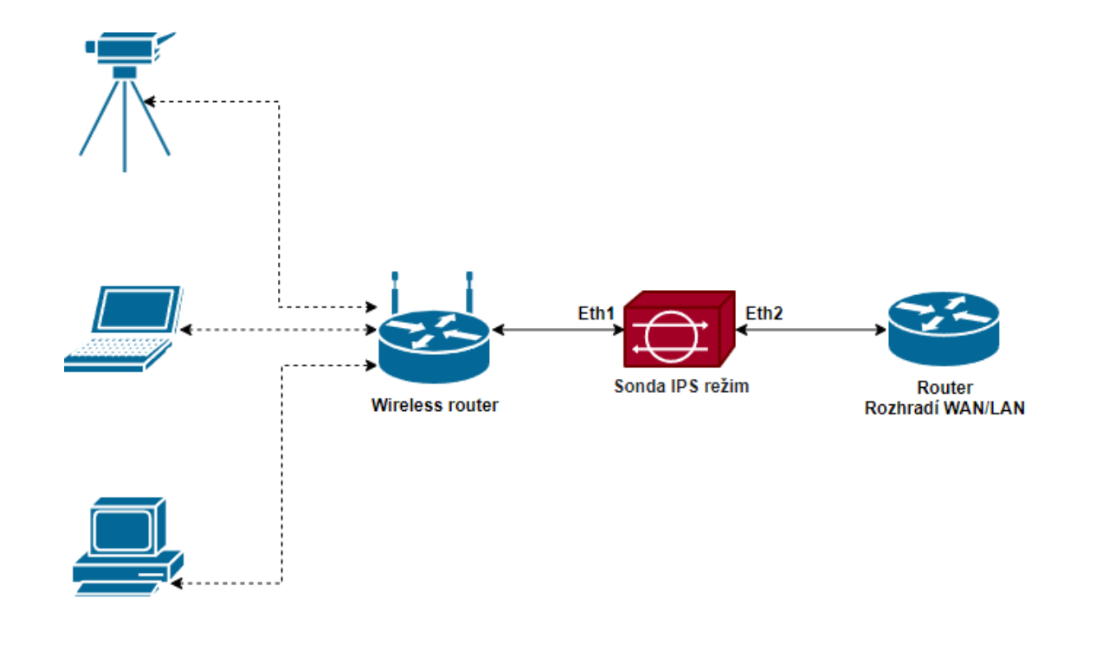
**Automatizované testy** - testy vytvořené experty v oboru.

**Semiautonomastizované testy** - hybrid předchozích dvou typů testů.

#### Analýza testované infrastruktury

Před navrhování samotných scénářů útoků je vhodné se zamyslet nad **typem infrastruktury**, kterou budeme testovat. Vyhodnotit, jaké technologie mohou mít slabým místem, jaká zařízení jsou do sítě připojené a na jaké oblasti bude [sonda SonIoT](https://soniot.fel.cvut.cz/) monitorovat.

Naše testovací síť obsahuje **sondu SonIoT** zapojenou v režimu *IPS (Intrusion Prevention Systems)*, počítač s Kali Linux a další zařízení.



Díky zapojení sondy v **režimu *IPS***bude procházet provoz skrze ní. Sonda by tak měla být schopna krom monitorování bezpečnostních hrozeb i filtrovat a zachytit blížící se útoky.

### Měření

*Vytížení sondy je měřeno dodatečně v režimu IDS. Vše ostatní v režimu IPS.*

#### 1. Zjištění služeb, které používá sonda

Abychom byli schopni efektivněji cílit útoky, snažili jsme se v prvním kroku analyzovat porty a konkrétní služby, které sonda využívá.

Na sondě jsme objevili pouze 2 služby. Konkrétně ssh, přes které jsme připojeni a tcp pomocí kterého je připojeno logování dat

Na sondě jsme nalezli pouze 2 služby na 2 portech. Konkrétně:

* na portu **22** službu **ssh**, která
* a na portu **3000** službu pro komunikaci s Mongodb.

##### Snippet kódu

nmap -sV 192.168.28.53 # map target ports

##### Screenshot



##### Hodnocení úspěšnosti

Tabulka vygenerovaných alertů - [port mapping](https://docs.google.com/spreadsheets/d/1mIYbll9a5Ht2oi13N3Dca-fqEf-K3ry2RtB6sKfKlzc/edit#gid=0)

Sonda správně vyhodnotila scan portů pomocí nmap, scan některých sportů vyhodnotila přímo pomocí alertu “ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)” ostatní pomocí alertů začínajícími “ET SCAN” pokračující typem “portů”:, na kterých je scan prováděn. Jedná se o různé typy SQL a poté také portů pro VNC.

##### Vytížení sondy

Při provádění tohoto testu jsme na sondě nezaznamenali žádné abnormální využití výpočetních prostředků.

#### 2. Slovníkový útok na login pomocí Metasploit

Jako první útok jsme zvolili naivní slovníkový útok na openSSH s využitím frameworku *Metasploit*.

##### Screenshot

##### Hodnocení úspěšnosti

Tabulka vygenerovaných alertů - [Metaspoit](https://docs.google.com/spreadsheets/d/1FUDuQkRhZW279CoB1FujLAHV-lan-SGeSEbBAwxWVzE/edit#gid=0)

Tento test sonda také vyhodnotila správně, pomocí alertu “ET SCAN Potential SSH Scan OUTBOUND”. Pouze při source portu se objevil alert spolu s předcházejícím i alert “ET SCAN Potential SSH Scan”. Tento postrádá “OUTBOUD”, předpokládáme tedy že zde se scan odhalil využívaný port.

##### Vytížení sondy

Při tomto testu je krásně viditelné zvýšení zatížení síťové karty sondy viz[network\_test2.PNG](https://drive.google.com/file/d/15Kmf6n6hDmVMcqOmVLFOOPQzk1Sk95z5/view?usp=share_link)(měření sítě zde muselo proběhnout dvakrát z důvodu chybného screenshotu). Změna je vidět i ve vytížení CPU[cpu\_test2.PNG](https://drive.google.com/file/d/1xsdq67MYBLKuVP5mUfD8f8IIgg7wOYPF/view?usp=share_link)

#### 

#### 3. Brute Force na SSH pomocí hydry

Druhým útokem jsme opět cílili na ***ssh****.* Tentokrát jsme s k útoku využili slovníkového útoku nástroje hydra.

##### Snippet kódu

hydra -l root -P tmp/rockyou.txt.gz 192.168.28.53 -t 4 ssh[[4]](#footnote-3)

##### Screenshot

##### Hodnocení úspěšnosti

Tabulka vygenerovaných alertů - [Hydra brute force](https://docs.google.com/spreadsheets/d/1VyaSNpYblgp2iCla2u8A5qGScdPCTWTo_oaz_EPhUmk/edit#gid=0)

Při tomto testu se dva ze sedmi alertů přímo týkají SSH bruteforce útoku. Jedná se o alert “ET SCAN LibSSH Based Frequent SSH Connections Likely BruteForce Attack”. Další dva jsou typu “ET SCAN Potential SSH Scan”, ty se také dalo očekávat při tomto útoku. Ovšem zbytek alertů je typu “GPL WEB\_SERVER DELETE attempt”, ty nejspíše nejsou při tomto útoku využívané a proto jsou chybné.

##### Vytížení sondy

Dle očekávání je na grafech jasně vidět zvýšená aktivita při testu.

[network\_test3.PNG](https://drive.google.com/file/d/1XaQy172eb0k-SjwrXL6eOAoQb0S3tRO0/view?usp=share_link) [cpu\_test3.PNG](https://drive.google.com/file/d/10fC6Y1zrZ2QcUzfTESamX_1QxEd1f7Yh/view?usp=share_link)

#### 4. Mapování zařízení v síti pomocí

V dalším kroku jsme chtěli zmapovat, jaká jiná zařízení jsou v síti. K tomu jsme využili opět nástroje ***nmap***.

##### Snippet kódu

nmap -v -sn 192.168.0.0/16 # mapuje zařízení v dané síti

##### Screenshot



##### Hodnocení úspěšnosti

Tabulka vygenerovaných alertů - [Mapovaní zařízení v síti](https://docs.google.com/spreadsheets/d/18i7eZ2PNunR2vkjwRrmg-0CZfdAS_Vfw2pgvnGspulM/edit#gid=0)

Při tomto útoku byly vygenerovány pouze alerty “GPL WEB\_SERVER DELETE attempt”

Výsledek ze sondy v tomto případě byl nesprávný, nejednalo se o pokus o smazání sondy, nýbrž pouze o mapování lokální sítě.

##### Vytížení sondy

Při tomto testu je vidět v grafech mírně zvýšená aktivita oproti normálu, ovšem není na takové úrovně aby šlo jistě určit že se jedná o jev způsobený testováním. Úrovně sondy při běhu bez testů dosti kolísají a dosahují i vyšších úrovní než zde zaznamenaných.[network\_test4.PNG](https://drive.google.com/file/d/15ibRAvtR9VcgPfYfdpLPhF4fCMCQ54qb/view?usp=share_link)[cpu\_test4.PNG](https://drive.google.com/file/d/1zX2TJp0cRSpAUOwYSIl75nnQ7cT935SQ/view?usp=share_link)

#### 

#### 5. Monkey HTTPD Header Parsing Denial of Service (DoS)

Dále jsme zkoušeli experimentovat s různými scénáři z frameworku ***Metasploit***. Vybrali jsme modul frameworku Metasploit s názvem Monkey HTTPD Header Parsing Denial of Service (DoS).

##### Popis scénáře

Tento modul způsobuje nesprávnou analýzu hlavičky, která vede k chybě segmentace kvůli speciálně vytvořenému požadavku HTTP. Ovlivňuje verzi <= 1.2.0.[[5]](#footnote-4)

##### Screenshot



##### Hodnocení úspěšnosti

15:28

Tabulka vygenerovaných alertů - [Monkey\_HTTPD(DoS)](https://docs.google.com/spreadsheets/d/1K0yFfxe7myY-QZVGHP3jZlQVYc6BHPeBBQ24m9RoQr4/edit#gid=0)

Při tomto testu sonda nejspíše vyhodnotila útok správně. Alerty které sonda vyhodnotila se všechny týkají HTTP, jedná se o “SURICATA HTTP Unexpected Request body” a “SURICATA HTTP unable to match response to request” . Sonda nevyhodnotila tuto činnost jako útok, nýbrž pouze jako neznámou a nečekanou aktivitu, kterou nemůže zpracovat.

##### Vytížení sondy

Zde jsme nezaznamenali žádné viditelné zvýšení. Dle typu testu se dá čekat, že se vytížení sondy znatelně nezmění.

#### 6. Mapovani portu na koncentratoru

Na závěr jsme se pokusili zmapovat porty a služby, které využívá koncentrátor, přes který se do sítě připojujeme.

##### Snippet kódu

nmap -Pn 192.168.28.15

##### Screenshot



##### Hodnocení úspěšnosti

Tabulka vygenerovaných alertů - [Mapovaní portů koncentrátoru](https://docs.google.com/spreadsheets/d/1a2mfkG3033fL6iGQ6ooBOu8YrRZjXnBSip5Cja8S1Js/edit#gid=0)

Zde opět sonda špatně vyhodnotila aktivitu na síti. Alerty, které za běhu tohoto testu sonda vyprodukovala, jsou všechny typu “GPL WEB\_SERVER DELETE attempt”. Stejně jako u mapování zařízení v síti.

##### Vytížení sondy

V tomto posledním testu i dle povahy testu samotného se neočekává zřetelné zvýšení aktivity na sondě a test prokázal správnost tohoto odhadu.

## Závěr práce

### Zhodnocení měření

Během měření se nám povedlo vygenerovat různé typy testů. Některé si kladly za cíl zmapovat cílovou infrastrukturu, jiné pomocí brute force útoku napadnout ssh službu. V návaznosti na typ sonda útok zachytila velice úspěšně.

### Zhodnocení spolupráce

Při práci na projektu jsme narazili na několik výzev, které nám práci ztížili. První byla naše neznalost problematiky síťové bezpečnosti a vhodných nástrojů. Poměrně dlouhou dobu nám zabralo najít vhodnou technologii a zprovoznit ji. Druhým problém byl způsoben naší nepozorností. Konkrétně tím, že jsme naměřili vše bez zaznamenání vytíženosti sondy. Proto jsme museli celé měření opakovat, abychom získali chybějící hodnoty.

Úkoly a odpovědnosti jsme si rozdělili následovně:

* Petr Kučera - studium problematiky penetračního testování a ovládání Kali Linux,
* Jan Tonner - analýza na úrovni sondy a následné zpracování dat,
* Petr Procházka - studium problematiky a analýza na úrovni sondy.

# Zdroje

## Literatura a reference

Dokumentace k Softwarovému Fraimeworku Metasploit: <https://docs.metasploit.com/>

Navo na praci s Metasploit: <https://nooblinux.com/metasploit-tutorial/>

Instalace Metasploit Framework: <https://www.kali.org/docs/tools/starting-metasploit-framework-in-kali/>

Přehlad zabuovaných nástrojů v Kali Linux: <https://www.kali.org/docs/tools/>

3 Penetrační test. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2022-10-28]. Dostupné z: <https://cs.wikipedia.org/wiki/Penetra%C4%8Dn%C3%AD_test>

1. T. Zitta et al., "Penetration Testing of Intrusion Detection and Prevention System in Low-Performance

   Embedded IoT Device," 2018 18th International Conference on Mechatronics - Mechatronika (ME), 2018, pp. 1-5. [↑](#footnote-ref-0)
2. SHIVAYOGIMATH, Chaitra N. An overview of network penetration testing. International Journal of

   Research in Engineering and Technology, 2014, 3.07: 5. [↑](#footnote-ref-1)
3. Penetrační test. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2022-10-28]. Dostupné z: <https://cs.wikipedia.org/wiki/Penetra%C4%8Dn%C3%AD_test> [↑](#footnote-ref-2)
4. Zdroj snippet kódu: <https://linuxconfig.org/ssh-password-testing-with-hydra-on-kali-linux> [↑](#footnote-ref-3)
5. Zdroj: <https://www.rapid7.com/db/modules/auxiliary/dos/http/monkey_headers/> [↑](#footnote-ref-4)