

Výzkum v oblasti kybernetické bezpečnosti

Den otevřené vědy 2025

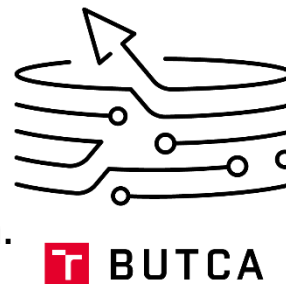
Willi Lazarov

Ústav telekomunikací, FEKT VUT v Brně

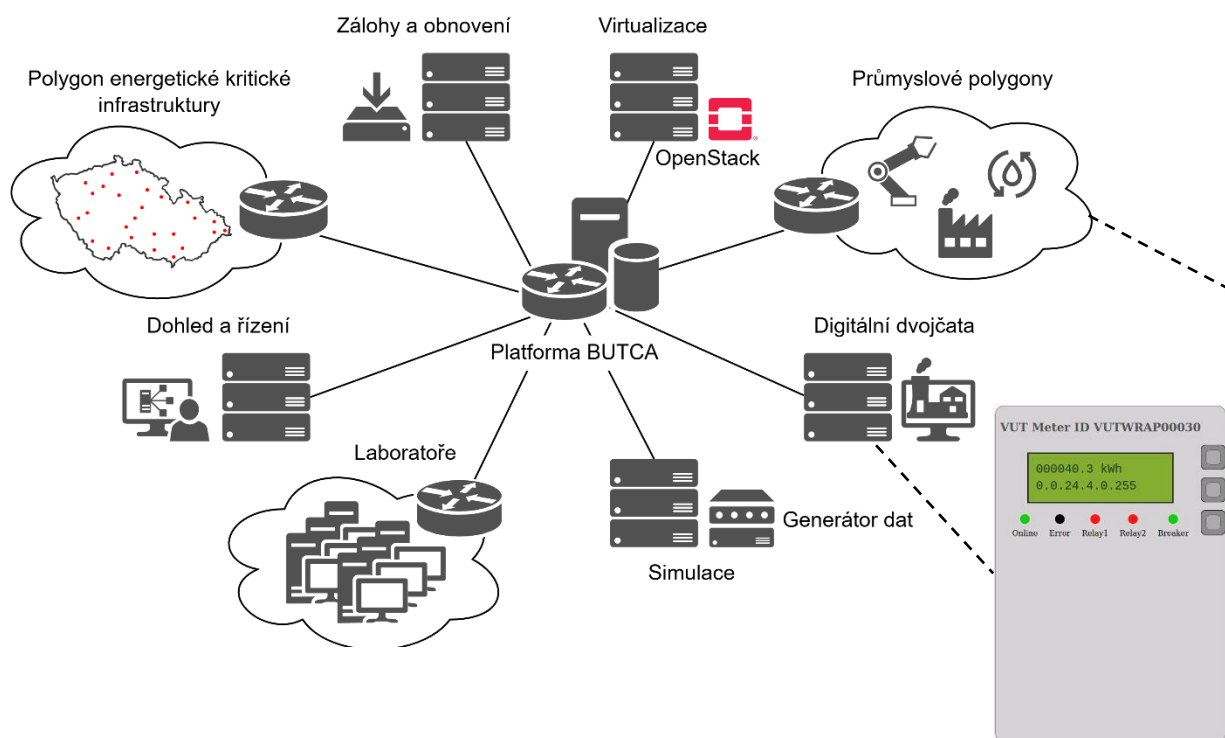
Strategické oblasti výzkumu – vzdělávání



- Vzdělávání v oblasti kybernetické bezpečnosti:
 - Simulace kybernetických hrozeb v izolovaném prostředí.
 - Interaktivní výuka, profilace učených osob a zpětná vazba.



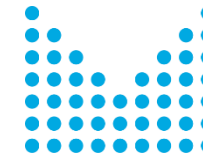
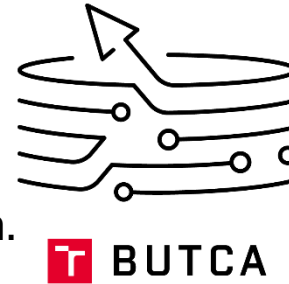
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



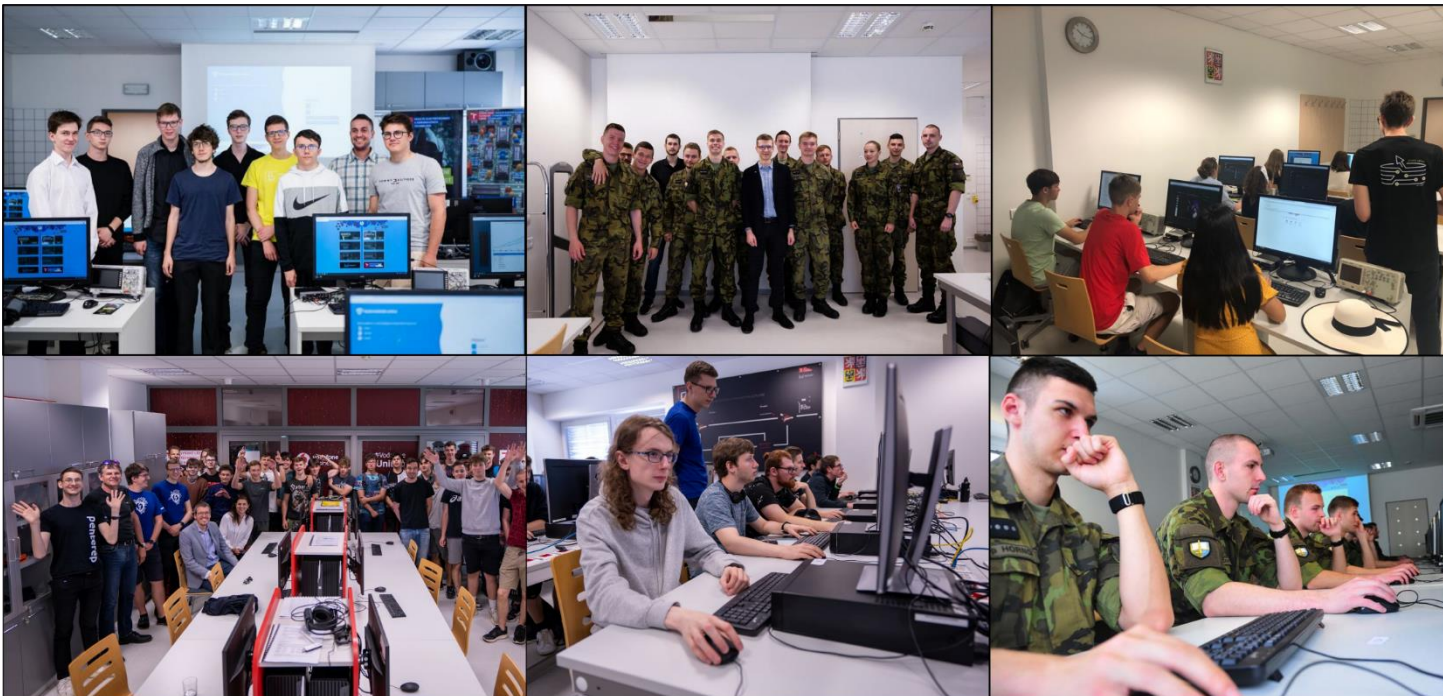
Strategické oblasti výzkumu – vzdělávání



- Vzdělávání v oblasti kybernetické bezpečnosti:
 - Simulace kybernetických hrozeb v izolovaném prostředí.
 - Interaktivní výuka, profilace učených osob a zpětná vazba.



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



Bezpečnost chytrých elektroměrů

Časový limit01 : 11 : 42

Úkol 4: Analýza komunikace

Úspěšným získáním hesla v otevřené podobě jste našli zvláštní zranitelnost. Než budete pokračovat dál, tak nezapomeňte vypnout ARP spoof. Samotné heslo vám však nestačí. V DIMS je totiž více parametrů spojení. Prohlédněte si zachycenou komunikaci ještě jednou a sestavte všechny parametry spojení.

1. K sestavení spojení je potřeba znát:

2. Asociální objekt (Association Object)

3. Adresu klienta (Client Address), někdy označována jako TargetAddress

4. Typ autentizace (Authentication)

5. Heslo (Password)

6. IP Adresu (Hostname)

7. Port

Nástroj Wireshark používaný v této úloze sice již má nainstalovaný LUA doplněk k překladači DIMS protokolu, avšak na všechny požadavky tento doplněk umí přeložit. Pro přesnější přeložení komunikace je potřeba komunikaci přeložit pomocí Gurus DIMS Translatoru, který se nachází na ploše, nebo zde na odkaz <https://www.gurus.fi/GurusDIMSTranslator>.

Tyto informace si uložte!

Správným řešením pro tento úkol je asociální objekt a adresa klienta oddělené podtržítkem. Odpověď zadejte ve tvaru: AsociálníObjekt_AdresaKlienta (např. 012345_10)

← Zpět

Zadání

Sandbox prostředí

Otevřít sandbox

Obnovit spojení

Správná odpověď (flag)

Zadejte flag

Odeslat Dp

10 bodů

Nápovědy k úkolu

Nápověda #1

Nápověda #2

Nápověda #3

Strategické oblasti výzkumu – vzdělávání



Univerzita obrany
v Brně



VOŠ a SPŠE
PLZEŇ



Střední průmyslová škola
a Střední odborná škola
Dvůr Králové nad Labem



Gymnázium, Ostrava-Hrabůvka



Strategické oblasti výzkumu – etický hacking



■ Etický hacking:

- Platforma a automatizované nástroje pro podporu penetračního testování.
- Bezpečnost webových aplikací, síťové infrastruktury a aplikačních služeb.



Vysoké učení technické v Brně

Brno University of Technology

cyberarena.utko.feec.vutbr.cz

Autentizace

Jméno a heslo

SMS kód (druhý faktor)

Lokální úložiště

PHPSESSID

lang

Session management

Software

Laravel

Vue.js

Ubuntu

Zdroje

/robots.txt

/index.php

query

/images/

Test

Websockety

Jméno a heslo

Informace

Testy

Označení↑↓	Úkol↑↓	Obt...↑↓	Stav↑↓	Nález↑↓
PTL-WEB-AUTH-PWSPA	Není zakázáno použít znak mezery v hesle?	Snadné	✓	✗
PTL-WEB-AUTH-PWREM	Nejsou z hesla vypouštěny mezery?	Snadné	—	—
PTL-WEB-AUTH-PWSPL	Nedochází ke slučování více po sobě jdoucích mezer do jednoho znaku?	Snadné	—	—
PTL-WEB-AUTH-PWTRI	Nedochází k ořezávání bílých znaků na začátku, nebo konci hesla?	Snadné	✓	✗
PTL-WEB-AUTH-PWCOD	Jsou mezery v hesle při přenosu správně kódovány a následně dekód...	Snadné	✓	—
PTL-WEB-AUTH-PWUNI	Je povoleno použít v hesle UNICODE znaky?	Snadné	✓	—
PTL-WEB-AUTH-PWINT	Jsou UNICODE znaky v hesle interpretovány správně jako jeden znak?	Snadné	✓	✗
PTL-WEB-AUTH-PWFAU	Neznemožní UNICODE znaky v hesle možnost ověření hesla?	Snadné	✓	✗
PTL-WEB-AUTH-PWCHG	Může si uživatel změnit své heslo?	Snadné	—	—
PTL-WEB-AUTH-PWINV	Je po změně hesla původní heslo zneplatněno?	Snadné	—	—

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Strategické oblasti výzkumu – OSINT

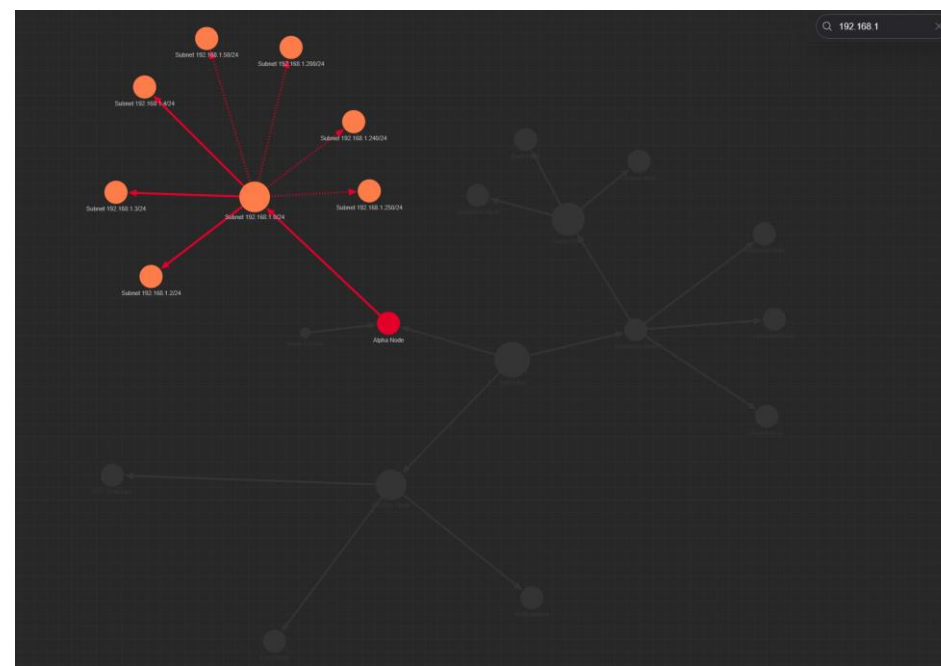
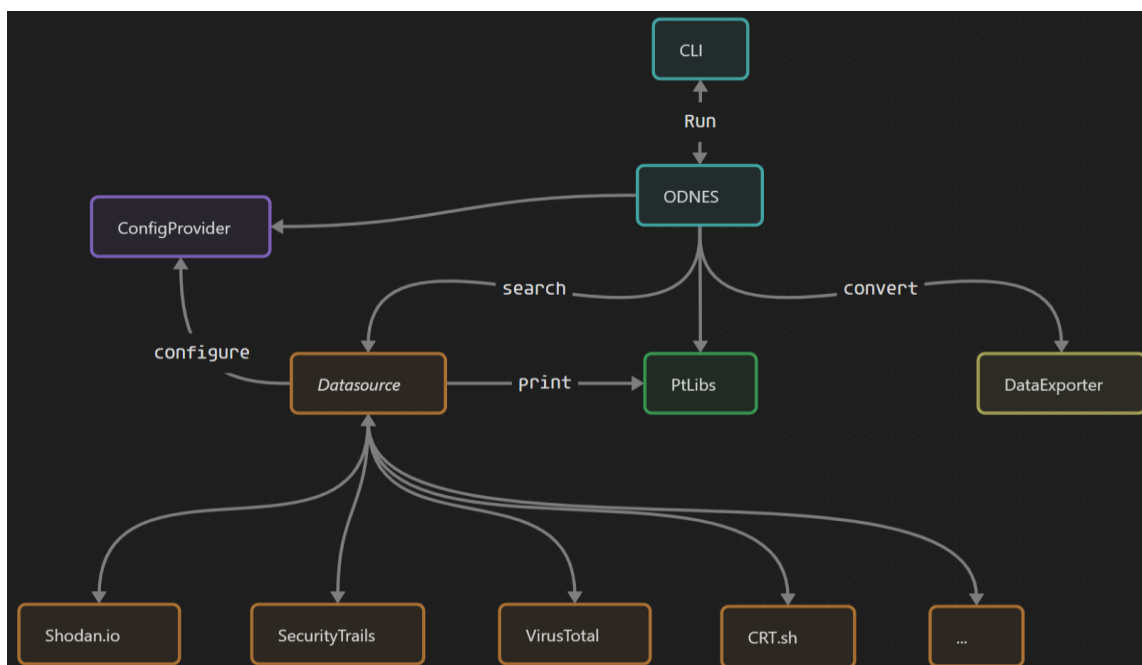


- Open source intelligence (OSINT):

- Podpůrné nástroje pro sběr dat z otevřených zdrojů.
- Interaktivní prostředí pro analýzu velkého objemu dat.
- Zpravodajská činnost, deanonymizace aktérů hrozeb atd.



VeInKyS AČR



Strategické oblasti výzkumu – hybridní hrozby



■ Boj proti hybridním hrozbám:

- Adaptivní monitoring hrozeb v kyberprostoru.
- Tematické modelování a analýza sentimentu.
- Identifikace trollích farem a vlivových operací.
- Spolupráce s Univerzitou obrany a Armádou ČR.

MINISTERSTVO OBRANY
ČESKÉ REPUBLIKY

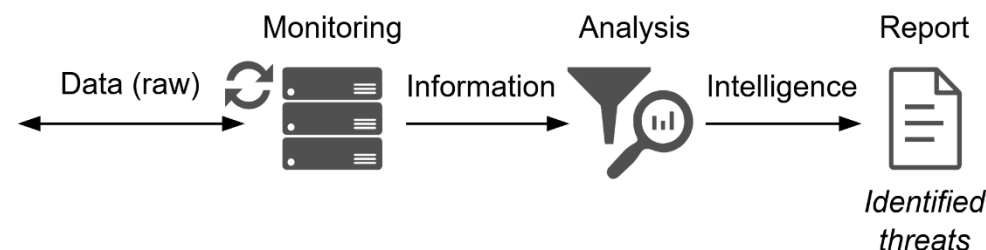
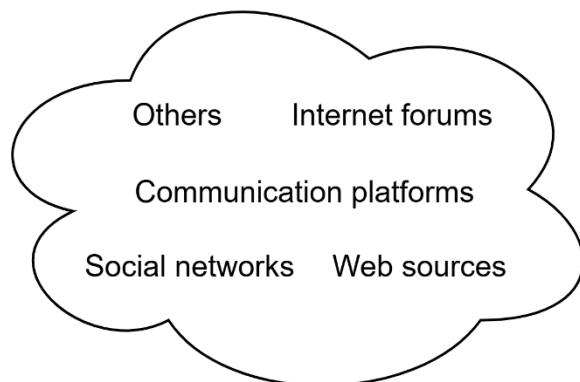


VeInKyS AČR



Univerzita obrany
v Brně

Cyberspace (open source data)



Děkuji za pozornost

Máte zájem o spolupráci? Kontaktujte nás na e-mail níže.

Willi Lazarov (lazarov@vut.cz)

Kontaktní osoba:

Zdeněk Martinásek (martinasek@vut.cz)

Ústav telekomunikací, FEKT VUT v Brně