KYPO - Analyst

Cílem analýzy je získat představu o **zaujetí hráčů** (engagement) - jak moc hráči byli aktivní při řešení bezpečnostních úkolů namísto pasivního čtení nápověd a opisování doporučených příkazů a jak se jejich zaujetí měnilo v průběhu cvičení.

Organizátoři průzkumu:

- doc. RNDr. Radek Ošlejšek, Ph.D.
- Bc. Vojtěch Malý
- Bc. Tomáš Kadavý

* Označuje povinnou otázku

1. **Souhlas se zpracováním dat** *

Souhlasím s účastí na experimentu, jehož cílem je ověřit praktickou použitelnost nástrojů pro analýzu chování hráčů bezpečnostních her v prostředí KYPO Cyber Range. Byl(a) jsem poučen(a), že data získaná z herního prostředí a odpovědi poskytnuté tímto dotazníkem budou anonymizována a použita výhradně pro vědecké účely.

Zaškrtněte všechny platné možnosti.

- [ ] Souhlasím se zpracováním dat

[15 min] Seznámení se s prostředím

Prohlédněte si instruktážní **video**. Souběžně si můžete GUI zkoušet v **demo aplikaci** (přístup povolen pouze ze sítě FI). Poté přejděte do další sekce.

Informace o hře (obsahu dat):

48 studentů hrálo mírně modifikovanou hru Locust 3302. Cvičení probíhalo pod dohledem cvičícího a časově bylo omezeno na dvě hodiny. Čísla a obsah herních úrovní (úkolů):

- 78. INFO LEVEL: Popis příběhu
- 33. INFO LEVEL: Instrukce ke cvičení
- **34. TRAINING LEVEL:** Student se má přihlásit na stroj s IP 10.1.135.83, oskenovat porty na serveru 172.18.1.5 pomocí *nmap* a zjistit tak běžící služby.
- **35. TRAINING LEVEL:** Vyhledání možných zranitelností běžících služeb, a to pomocí Googlu nebo nástroje *metasploit*.
- **36. TRAINING LEVEL:** Použití *metasploit* k využití zranitelnosti jedné ze služeb k získání přístu k serveru.
- **37. TRAINING LEVEL:** Prozkoumání souborového systému serveru, analýza *.bash_history* s cílem najít záložní server, na který útočník zkopíroval data (je to stroj s IP 10.1.17.4).
- **38. TRAINING LEVEL:** Prolomení SSH klíče pomocí nástroje *john*.
- 39. INFO LEVEL: Blahopřání k úspěšnému dokončení.
- 40. INFO LEVEL: Zpětná vazba.

[40 min] Uživatelské testování

Pokyny:

- **Zavřete demo aplikaci**, aby se nepletla do následujícího testování.
- **Otevřete si ostrou aplikaci** s daty určenými pro uživatelské testování (přístup povolen pouze ze sítě FI)
- **Vyplňte základní údaje.**
- **Splňte úkoly** popsané v následujících sekcích a odpovězte na položení otázky. **Komentujte své myšlenky nahlas.** Nebojte se ptát. Neostýchejte se dávat negativním hodnocením.

Informace o hře (obsahu dat):

52 studentů hrálo mírně modifikovanou hru Locust 3302 (podobně jako u demo aplikace). Příběh byl ale adaptován na vnitřního útočníka (insider attack) a poslední úkol (prolamování SSH klíče) byl vynechán. Čísla a obsah herních úrovní (úkolů):

- 62. INFO LEVEL: Dotazník
- 42. INFO LEVEL: Instrukce ke cvičení
- **43. TRAINING LEVEL:** Student se má přihlásit na stroj s IP 10.1.135.83, oskenovat porty na serveru 172.18.1.5 pomocí *nmap* a zjistit tak běžící služby.
- **44. TRAINING LEVEL:** Vyhledání možných zranitelností běžících služeb, a to pomocí Googlu nebo nástroje *metasploit*.
- **45. TRAINING LEVEL:** Použití *metasploit* k využití zranitelnosti jedné ze služeb k získání přístu k serveru.
- **46. TRAINING LEVEL:** Prozkoumání souborového systému serveru, analýza *.bash_history* s cílem najít záložní server, na který útočník zkopíroval data (je to stroj s IP 10.1.17.4).
- 49. INFO LEVEL: Blahopřání k úspěšnému dokončení.

2. Pracovní pozice *

3. Moje zkušenost s účastí na kybercvičeních (jako hráč, KYPO i jiné) *

Označte jen jednu elipsu.

	1	2	3	4	5	
žádn	◯	◯	◯	◯	◯	vysoká (4 a více)

4. Počet cvičení, které jsem KYPO CRP přímo organizoval *

5. Moje zkušenost s analýzou výsledků bezpečnostních cvičení a přípavou zpětné vazby studentům (nejen v rámci KYPO)

Označte jen jednu elipsu.

	1	2	3	4	5	
žádr	◯	◯	◯	◯	◯	vysoká

6. Moje zkušenost s analytickým rozhraním v KYPO CRP

Označte jen jednu elipsu.

	1	2	3	4	5	
žádr	◯	◯	◯	◯	◯	vysoká

Identifikujte hráče (jednoho nebo více), kteří vykazují následující zaujetí. Zapište jejich ID do formuláře. Pokud žádný hráč s danou charakteristikou v datech není, zapište pomlčku:

7. Hráči s nízkým zaujetím během celého cvičení: *

8. Hráči s vysokým zaujetím během celého cvičení: *

9. Hráči, kteří během hraní zaujetí evidentně ztratili: *

10. Hráči, kteří během hraní zaujetí evidentně získali: *

11. Které části aplikace považujete pro daný úkol za užitečné: *

Zaškrtněte všechny platné možnosti.

- [ ] graf průchodů -- varianta frequency graph (uprostřed, defaultní zobrazení)
- [ ] graf průchodů -- varianta performance graph (uprostřed, po přepnutí)
- [ ] graf zaujetí -- varianta čárového grafu (vpravo nahoře, defaultní zobrazení)
- [ ] graf zaujetí -- varianta radarového grafu (vpravo nahoře, popřepnutí)
- [ ] heatmapa příkazů (vpravo dole)
- [ ] filtrování -- dočasné potlačení zobrazení hráčů a příkazů (temporary filtering vlevo)
- [ ] filtrování -- zdrojových dat (raw data filtering vlevo)

12. Jak snadné bylo splnit tento úkol *

Označte jen jednu elipsu.

	1	2	3	4	5	
Jedı	◯	◯	◯	◯	◯	Těžké

13. Volný komentář k úkolu:

Vyberte jednoho z hráčů, u kterého došlo ke zjevné ztrátě zaujetí až během hraní (viz první úkol). Ověřte hypotézu, že příčinou byl **nedostatek času**. Zaměřte se přitom na reálnou činnost hráče, tj, jaké příkazy používal, jestli si bral nápovědu apod.

14. ID vybraného hráče *

15. Příčinou byly nedostatatek času

Označte jen jednu elipsu.

	1	2	3	4	5	
Veln	◯	◯	◯	◯	◯	Velmi pravděpodobné

16. Které části aplikace považujete pro daný úkol za užitečné: *

Zaškrtněte všechny platné možnosti.

- [ ] graf průchodů -- varianta frequency graph (uprostřed, defaultní zobrazení)
- [ ] graf průchodů -- varianta performance graph (uprostřed, po přepnutí)
- [ ] graf zaujetí -- varianta čárového grafu (vpravo nahoře, defaultní zobrazení)
- [ ] graf zaujetí -- varianta radarového grafu (vpravo nahoře, popřepnutí)
- [ ] heatmapa příkazů (vpravo dole)
- [ ] filtrování -- dočasné potlačení zobrazení hráčů a příkazů (temporary filtering vlevo)
- [ ] filtrování -- zdrojových dat (raw data filtering vlevo)

17. Jak snadné bylo splnit tento úkol *

Označte jen jednu elipsu.

	1	2	3	4	5	
Jedı	◯	◯	◯	◯	◯	Těžké

18. Volný komentář k úkolu, zdůvodnění výsledku:

Pro stejného hráče, jako v předchozím úkolu, ověřte hypotézu, že příčinou ztráty zaujetí byly **nedostatečné vstupní znalosti**. Případně formulujte a prověřte vlastní hypotézy. Zaměřte se přitom na reálnou činnost hráče, tj, jaké příkazy používal, jestli si bral nápovědu apod.

19. Příčinou byly nedostatečné znalosti:

Označte jen jednu elipsu.

	1	2	3	4	5	
Veln	◯	◯	◯	◯	◯	Velmi pravděpodobné

20. Které části aplikace považujete pro daný úkol za užitečné: *

Zaškrtněte všechny platné možnosti.

- [ ] graf průchodů -- varianta frequency graph (uprostřed, defaultní zobrazení)
- [ ] graf průchodů -- varianta performance graph (uprostřed, po přepnutí)
- [ ] graf zaujetí -- varianta čárového grafu (vpravo nahoře, defaultní zobrazení)
- [ ] graf zaujetí -- varianta radarového grafu (vpravo nahoře, popřepnutí)
- [ ] heatmapa příkazů (vpravo dole)
- [ ] filtrování -- dočasné potlačení zobrazení hráčů a příkazů (temporary filtering vlevo)
- [ ] filtrování -- zdrojových dat (raw data filtering vlevo)

21. Jak snadné bylo splnit tento úkol *

Označte jen jednu elipsu.

	1	2	3	4	5	
Jedı	◯	◯	◯	◯	◯	Těžké

22. Volný komentář k úkolu, zdůvodnění výsledku, další hypotézy:

_____

Zhodnoťte celkový průběh cvičení. Ověřte následující hypotézy.

23. Většina hráčů měla a udržela si vysoké zaujetí hrou. *

Označte jen jednu elipsu.

	1	2	3	4	5	
Soul	◯	◯	◯	◯	◯	Nesouhlasím

24. Slovní zdůvodnění:

_____

25. Časový limit cvičení byl v pořádku (nezpůsobil ve vělké míře pokled zaujetí v důsledů časového presu) *

Označte jen jednu elipsu.

	1	2	3	4	5	
Soul	◯	◯	◯	◯	◯	Nesouhlasím

26. Slovní zdůvodnění:

_____

27. Které části aplikace považujete pro daný úkol za užitečné: *

Zaškrtněte všechny platné možnosti.

- [ ] graf průchodů -- varianta frequency graph (uprostřed, defaultní zobrazení)
- [ ] graf průchodů -- varianta performance graph (uprostřed, po přepnutí)
- [ ] graf zaujetí -- varianta čárového grafu (vpravo nahoře, defaultní zobrazení)
- [ ] graf zaujetí -- varianta radarového grafu (vpravo nahoře, popřepnutí)
- [ ] heatmapa příkazů (vpravo dole)
- [ ] filtrování -- dočasné potlačení zobrazení hráčů a příkazů (temporary filtering vlevo)
- [ ] filtrování -- zdrojových dat (raw data filtering vlevo)

28. Jak snadné bylo splnit tento úkol *

Označte jen jednu elipsu.

	1	2	3	4	5	
Jedı	◯	◯	◯	◯	◯	Těžké

29. Volný komentář k úkolu:

[5 min] System Usability Scale (SUS)

Tato poslední sada otázek má za cíl obecně zhodnotit použitelnost GUI. Protože se jedná o standardní dotazník, jsou otázky v angličtině.

30. I think that I would like to use this visualization tool frequently. *

Označte jen jednu elipsu.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

31. I found the visualization tool unnecessarily complex. *

Označte jen jednu elipsu.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

32. I thought the visualization tool was easy to use. *

Označte jen jednu elipsu.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

33. I think that I would need the support of a technical person to be able to use this visualization tool. *

Označte jen jednu elipsu.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

34. I found the various functions in this visualizations tool were well integrated. *

Označte jen jednu elipsu.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

35. I thought there was too much inconsistency in this visualization tool. *

Označte jen jednu elipsu.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

36. I would imagine that most people would learn to use this visualization tool very quickly. *

Označte jen jednu elipsu.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

37. I found the visualization tool very awkward to use. *

Označte jen jednu elipsu.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

38. I felt very confident using the visualization tool. *

Označte jen jednu elipsu.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

39. I needed to learn a lot of things before I could get going with this visualization tool. *

Označte jen jednu elipsu.

	1	2	3	4	5	
Stro	◯	◯	◯	◯	◯	Strongly Agree

Obsah není vytvořen ani schválen Googlem.