Slovenská technická univerzita v Bratislave

Fakulta informatiky a informačných technológií

Ilkovičova 2, 842 16 Bratislava 4

**Inžinierske dielo**

*CYRAN*

Tím 19: Perdek, Karakaš, Matovič, Spusta, Saleh, Balga

Študijný program: Informatika Ročník: 4. Predmet: Tímový projekt Vedúci projektu: Ing. Pavol Helebrandt Phd.

**Požiadavky riešenia**

Podľa zadania a následných konzultácií s product ownerom boli identifikované nasledovné požiadavky riešenia:

* Navrhnúť simulačné prostredie spolu s vybranými scenármi pre testovanie kybernetickej ochrany
* Použiť platformu (simulačného prostredia) pre realizáciu tohto prostredia (Odporúčanie použiť KYPO)
* Tvorba simulačného prostredia na jednom fyzickom PC pomocou viacerých virtuálnych strojov

**Scenáre**

* Otestovať už existujúce scenáre
* Navrhnúť 2-3 vlastné scenáre vhodné do výučby na FIIT
* Implementovať navrhnuté prostredie a scenáre na prostriedkoch FIIT
* Otestovať navrhnuté prostredie a scenáre na prostriedkoch FIIT
* Scenáre by mali slúžiť na podporu a zlepšenie výučby predmetov informačnej a sieťovej bezpečnosti.
* Identifikácia vhodných typov scenárov pre zapracovanie do problematiky
* Identifikácia vhodných typov problémov pre zapracovanie do scenárov
* Scenáre by mali zaujať hráča
* Zakomponovanie špeciálnych vlastností virtuálnych systémov s dôrazom na ich vplyv na existujúce a aj nové zraniteľnosti a detekcie (resp. prevencie prienikov zneužívajúcich tieto zraniteľnosti)
* Obsahom scenárov by malo byť zabezpečenie rôznych systémov ako aj rôzne prieniky do nich

**Nasadenie**

* Nasadenie výsledného riešenia pomocou virtuálnych strojov
* Nasadenie simulačného prostredia v prostredí OpenStack
* Nasadenie výsledného riešenia s minimalizáciou manuálnych úkonov a zásahov zo strany pedagóga

**Nefunkcionálne požiadavky**

* Riešenie by malo byť dynamicky škálovateľné podľa aktuálnych potrieb a dostupných prostriedkov

**Big Picture**

**Úvod**

Cyran projekt je zameraný na možnosť zlepšenia a testovania svojich schopností v simulovanej realite kyberpriestoru. Účastníci riešia rôzne úlohy a snažia sa odvrátiť útoky alebo sa infiltrovať do počítača cudzej osoby, prípadne podniknúť inú formu útoku. Cieľom je nájsť potencionálnu zraniteľnosť systému pre tím, ktorý sa obraňuje, prípadne získať informáciu v najčastejšie v podobe textového reťazca od brániaceho sa tímu.

**Ciele**

V rámci projektu je naším hlavným cieľom zostrojiť aplikáciu využívajúcu platformu KYPO, ktorá by používateľom umožnila vzdelať a súperiť v oblasti kybernetickej ochrany formou vytvorených hier. Každá hra bude založená na originálnom scenári pre otestovanie a prípadne aj naučenie používateľa rôznym technikám, na ktoré bude orientovaný. Ďalšími vedľajšími cieľmi, ktoré poslúžia pre realizáciu hlavného cieľa alebo napĺňajú novú funkcionalitu, ktorá podporuje požiadavky riešenia sú:

* Použitie platformy KYPO pri realizácii aplikácie ako aktualizovaného prostredia
* Analýza problematiky kybernetickej bezpečnosti
* Návrh scenárov zameraných na špeciálne situácie akými sú chyby v systéme alebo oboznámenie sa z rôznymi nástrojmi
  + Tieto scenáre budú mať edukatívny charakter
  + Nápovedy by mali slúžiť pre ponorenie používateľa do problému
  + Herný systém by mal identifikovať schopnosti a úroveň hráča pre lepší herný zážitok a poučenie z hry
  + Akcie používateľa by sa mali zaznamenávať pre identifikáciu rôznych návykov
  + Overenie na základe dotazníkov a rozhovorov by malo slúžiť na hľadanie vhodného scenáru pre konkrétnu problematiku
  + Analýza novo nájdených zraniteľností
  + Automatizácia procesov vyhodnocovania priebehu hry
    - Rozhodnutie ktoré schváli koordinátor
    - Automatické rozhodovanie
* Tvorba docker image-ov pre jednoduché nasadenie aplikácie
* Nasadenie aplikácii na OpenStack ako želaného miesta
* Dôraz pri návrhu a implementácii na objektové prístupy, architektúru s podpory interoperability a rozšíriteľnosti riešenia

**Ohraničenia**

Ohraničenia, ktoré náš systém bude mať budú počet realizovaných scenárov a overenia s konkrétnymi študentmi pre dĺžku trvania projektu.

**Globálne ciele na zimný semester**

Globálne ciele na zimný semester sú

* Použitie platformy KYPO pri realizácii aplikácie ako aktualizovaného prostredia
* Analýza problematiky kybernetickej bezpečnosti
* Návrh scenárov zameraných na špeciálne situácie akými sú chyby v systéme alebo oboznámenie sa z rôznymi nástrojmi
  + Tieto scenáre budú mať edukatívny charakter
  + Nápovedy by mali slúžiť pre ponorenie používateľa do problému
  + Herný systém by mal identifikovať schopnosti a úroveň hráča pre lepší herný zážitok a poučenie z hry
  + Akcie používateľa by sa mali zaznamenávať pre identifikáciu rôznych návykov
  + Overenie na základe dotazníkov a rozhovorov by malo slúžiť na hľadanie vhodného scenáru pre konkrétnu problematiku
  + Analýza novo nájdených zraniteľností
  + Automatizácia procesov vyhodnocovania priebehu hry
    - Rozhodnutie ktoré schváli koordinátor
    - Automatické rozhodovanie
* Tvorba docker image-ov pre jednoduché nasadenie aplikácie
* Dôraz pri návrhu a implementácii na objektové prístupy, architektúru s podpory interoperability a rozšíriteľnosti riešenia

**Celkový pohľad na systém**

**Moduly systému**

Moduly systému sú

**Príručky**

Príručky

**Technická dokumentácia**

Technická dokumentácia