Projekt: Laboratórium Kybernetickej Bezpečnosti

Popis projektu:

Laboratórium Kybernetickej bezpečnosti je technologické prostredie vytvorené na vzdelávanie a výskum v oblasti kybernetickej bezpečnosti. Jeho úlohou je zabezpečiť prostredie s možnosťou:

- simulácie reálnych útokov na IT infraštruktúru,
- testovanie jednotlivých spôsobov ochrany,
- vývoja spôsobov ochranných opatrení na nové útoky,
- vývoja nových aplikácií a zariadení voči kybernetickým hrozbám,
- vytvoriť nový študijní odbor,
- vzdelávanie väčšej skupiny a možnosťou individuálneho prístupu,
- využívania pre pedagógov, študentov, doktorandov a komerčné školenia

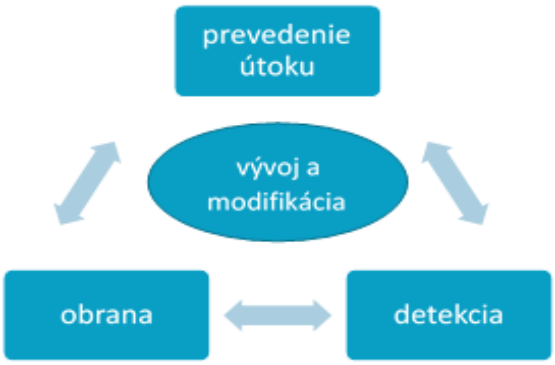
Laboratórium Kybernetickej bezpečnosti musí byť technologicky zabezpečené tak, aby svojou prevádzkou neohrozoval zvyšnú časť školskej infraštruktúry.

Fungovanie laboratória je založené na dôslednom zvládnutí:

- jednotlivých častí rizikových vektorov a možnosti ich kombinácie pre úspešný prienik
- obranných mechanizmov
- vývoja nových postupov na ochranu IT infraštruktúry.

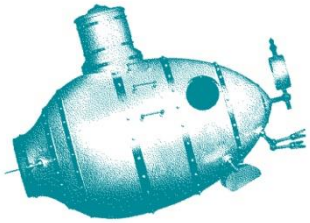
Kybernetická bezpečnosť je stály proces v ktorom sa na jednej strane útočníci snažia nájsť a využiť zraniteľné miesta IT infraštruktúry a na druhej strane sa vyvíjajú spôsoby ich detekcie a obrany.

Životný cyklus útoku



Kybernetické laboratórium má technologicky zabezpečiť zvládnutie celého životného cyklu útoku:

- vysvetlenie problematiky
- praktické prevedenie útoku
- detekcia útoku
- obrana voči útoku
- vývoj nových možností útokov a obranných mechanizmov
- otestovanie funkčnosti zmien



Príklady tém:

1) Skenovanie sietí
   a) nmap, unicornscan, hping, idle scan, ARP
2) Sociálne inžinierstvo
   a) sociálne techniky,
   b) falošné webové stránky,
   c) Spear phishing, vishing
   d) deployment malwaru
3) Pokročilejšie útoky
   a) Využitie Metasploit Framework pre exploitáciu sieťových služieb
   b) Vytváranie vlastnej Botnet siete
   c) Steganografia a rootkity
   d) MitM a obchádzanie HTTPS zabezpečenia
4) Hacking Web Serverov
   a) DoS a DDoS,
   b) Bruteforcing,
   c) klonovanie,
5) Hacking webových aplikácií
   a) mapovanie aplikácií,
   b) XSS, CSRF, RFI, LFI,
   c) hidden field manipulation
6) Bezdrôtové siete
   a) Druhy rámcov používaných v bezdrôtových sieťach
   b) Analýza bezdrôtových sietí v dosahu
   c) Zneužitie neautorizovaných rámcov
   d) WiFi Injection a monitor mód WiFi kariet
   e) Útoky na WEP siete, WPA1 PSK a WPA2 PSK siete
   f) Prelamovanie EAPOL rámcov pomocou grafických kariet
   g) Votrelecká AP
7) Mobilné zariadenia a ich aplikácie
8) Správa hesiel a možnosti ich krádeže

Kybernetické laboratórium pomôžeme napĺňať výzvy spojené s novými kybernetickými hrozbami a právnymi predpismi týkajúce sa rozvoja Kybernetickej bezpečnosti.