UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
PRÍRODOVEDECKÁ FAKULTA

VÝUČBA INFORMAČNEJ BEZPEČNOSTI POMOCOU HONEYPOTOV

2016 **Bc. Anna LIPTAJOVÁ**

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
PRÍRODOVEDECKÁ FAKULTA

VÝUČBA INFORMAČNEJ BEZPEČNOSTI POMOCOU HONEYPOTOV

DIPLOMOVÁ PRÁCA

Študijný program:	Učiteľstvo slovenského jazyka a literatúry a informatiky
Pracovisko:	Ústav informatiky
Vedúci diplomovej práce:	JUDr. RNDr. Pavol Sokol, PhD.
Konzultant diplomovej práce:	PaedDr. Ján Guniš, PhD.

Košice 2016

Bc. Anna LIPTAJOVÁ

Abstrakt v štátnom jazyku

Informácie sú všade okolo nás. Sú neoddeliteľnou súčasťou nášho života nášho každodenného života, preto majú pre nás vysokú, niekedy až nevyčísliteľnú hodnotu. Informačné systémy, ktorých úlohou je spracovávať informácie, sú často ľahkým cieľom útočníkov. Tí sa snažia informácie zneužiť vo vlastný prospech alebo použiť proti nám. Preto by sme sa mali naučiť tieto informácie chrániť. Ochrana informácií a informačných systémov je jedným z hlavných cieľov informačnej bezpečnosti. Existuje viacero prístupov, ktoré sa snažia predísť bezpečnostným útokom. Jedným z nich je aj použitie honeypotov. Honeypoty sú informačné systémy, ktoré priťahujú potencionálnych útočníkov svojou atraktívnosťou. Namiesto toho, aby sme útočníkovi bránili v jeho činnosti, umožníme mu uskutočniť útok na zariadení, pomocou ktorého môžeme dôkladne sledovať jeho postup či použité nástroje. Takto získané údaje nám poslúžia na odhaľovanie zraniteľností informačných systémov a analýzu rizík či bezpečnostných hrozieb. V rámci učebných plánov stredných škôl sa v informačnej bezpečnosti poskytuje len obmedzený priestor. Žiaci často využívajú rôzne sieťové služby, neuvedomujú si však potencionálne ohrozenie či riziko ich použitia. V tejto práci sme navrhli metodiku výučby informačnej bezpečnosti prostredníctvom honeypotov. Zamerali sme sa na bezpečnosť vybraných sieťových služieb cieľom naučiť žiakov základné pojmy informačnej bezpečnosti, Pripravili sme testovacie prostredie a iné didaktické pomôcky vhodné na vyučovanie informačnej bezpečnosti, ktoré sme overili v pedagogickej praxi.

Abstrakt v cudzom jazyku

Information is all around us. Information is an integral part of our daily lives, is valuable and very important for our society. Information systems process the information, but they are often an easy target for attackers. Attackers are trying to misuse the information for their own benefit or to use against us. Therefore, we should learn to protect our information. Protection of information and information systems is one of the main goals of information security. There are several approaches that seek to prevent security attacks. One of them is the use of honeypots. Honeypots are information systems that attract potential attackers its attractiveness. Instead of defence against attackers, honeypots allow him to carry out an attack. Honeypots will closely monitor the process and tools used by attackers. Honypot will serve us to detect vulnerabilities of information systems and risk analysis of security threats. Information security often has a limited space as a part in the schools´ curriculum. Students often use a variety of network services, but they do not realize the potential danger or risk of their use. In this paper we propose a methodology of teaching information security through a honeypot. We focused on the safety of selected network services in order to teach students the basic concepts of information security, we have prepared a test environment and other teaching aids suitable for the teaching of information security, which has been verified in educational practice.

Obsah

Zoznam ilustrácií

Zoznam tabuliek

Zoznam grafov

Zoznam skratiek a značiek

DoS Denial of Service

DDoS Distributed Denial of Service

IKT Informačno – komunikačné technológie

IP Internet Protocol

IPv6 Internet Protocol version 6

IS Information System

ISMS Information Security Management System

IŠVP Inovovaný štátny vzdelávací program

ŠVP Štátny vzdelávací program

ŠkVP Školský vzdelávací program

Slovník termínov

Informačná bezpečnosť je multidisciplinárna oblasť, ktorej úlohou je chrániť informácie, podieľať sa na skúmaní bezpečnostných hrozieb a navrhovať vhodné metódy na ochranu a prevenciu pred bezpečnostným útokom.

Honeypot je informačný systém, ktorého úlohou je prilákať útočníka aby uskutočnil bezpečnostný útok a následne zaznamenať všetky jeho kroky a prostriedky, ktoré útočník použil k bezpečnostnému útoku.

Honeynet je riadená sieť honeypotov, ktorá dokáže zaznamenať veľké množstvo dát a informácií o útočníkovi.

Malvér je zovšeobecňujúci pojem, ktorý označuje škodlivý softvér. Každý softvér, ktorý spôsobuje škodu pre používateľa informačného systému, pre počítač či počítačovú sieť, môžeme označiť ako malvér.

Úvod

Informácie sú dôležitou súčasťou informačnej spoločnosti. Na vytváranie, ukladanie a spracovávanie informácií používame informačné systémy a moderné informačno-komunikačné technológie, ktoré však môžu byť častým cieľom útočníka. Úlohou informačnej bezpečnosti je chrániť informácie, ktoré sú aktívom informačnej spoločnosti. Informačnú bezpečnosť môžeme pokladať za multidisciplinárnu oblasť, jej úlohou je taktiež skúmanie bezpečnostných hrozieb, vyhodnocovanie bezpečnostných rizík, definovanie bezpečnostnej politiky a navrhovanie vhodných metód ochrany a prevencie pred bezpečnostným útokom. Súčasťou informačnej bezpečnosti sú aj ľudia, ktorí pracujú s informáciami. Preto je dôležité rozširovať povedomie o informačnej bezpečnosti v celej spoločnosti.

Medzi inovatívne prístupy v informačnej bezpečnosti patrí aj použitie honeypotov. Honeypot je informačný systém, ktorého hlavnou úlohou je prilákať pozornosť útočníka. Honeypot vystupuje ako dôveryhodný a atraktívny zdroj informácií. Útočník, ktorý sa rozhodne zaútočiť na takýto systém však netuší, že honeypot podrobne zaznamenáva všetky kroky, ktoré útočník v rámci útoku podnikne. Dáta, ktoré nám honeypot poskytne majú veľký význam v kontexte informačnej bezpečnosti. Vďaka nim vieme vhodne ošetriť zraniteľnosti informačného systému, vhodne definovať pravidlá bezpečnostnej politiky a takto úspešne predchádzať bezpečnostným útokom.

Informačná bezpečnosť taktiež dôležitou súčasťou vyučovania informatiky na stredných školách. Štátny vzdelávací program definuje výkonové a obsahové štandardy pre žiakov stredných škôl. Žiaci by mali byť po absolvovaní predmetu schopní posúdiť základné riziká pri práci s počítačom, mali by vedieť rozpoznať počítačovú kriminalitu. Často sa však stáva, že informačnej bezpečnosti je v rámci vyučovania informatiky pridelená len minimálna pozornosť. Žiaci vedia definovať nebezpečný softvér, ale často majú problém predstaviť si ako v skutočnosti prebieha bezpečnostný útok.

V tejto práci použijeme honeypoty ako didaktické pomôcky, ktoré pomôžu študentom stredných škôl lepšie pochopiť základné pojmy informačnej bezpečnosti. Naším cieľom je nielen analyzovať využitie honeypotov pri výučbe informačnej bezpečnosti, ale aj vytvoriť a overiť metodiku vyučovania informačnej bezpečnosti prostredníctvom honeypotov. V práci navrhneme niekoľko modulov týkajúcich sa informačnej bezpečnosti, každý z modulov bude obsahovať výkonové a obsahové štandardy, didaktický materiál, nakonfigurovaný honeypot pripravený na použitie a v neposlednom metodiku výučby.

V prvej kapitole tejto práce sa budeme venovať samotnej informačnej bezpečnosti, priblížime si základné metódy a postupy ktoré využíva, definujeme si základné pojmy týkajúce sa informačnej bezpečnosti. Zároveň sa pokúsime upozorniť na dôležité miesto informačnej bezpečnosti vo výučbe informatiky na stredných školách a gymnáziách v rámci SR. V druhej kapitole sa zameriame na definovanie honeypotu ako didaktickej pomôcky vhodnej na výučbu informačnej bezpečnosti. Predstavíme si niektoré kategórie honeypotov a analyzujeme možnosti ich využitia vo výučbe. Tretia kapitola opisuje tvorbu laboratória informačnej bezpečnosti, ktoré budeme využívať vo výučbe. V rámci štvrtej kapitoly sú uvedené vytvorené didaktické moduly zamerané na výučbu konkrétnych pojmov informačnej bezpečnosti. Každý modul obsahuje metodiku a odporúčania pre učiteľov, ktoré sme zostavili na základe praktických skúseností z výučby vytvorených metodík.

1 Informačná bezpečnosť a jej výučba

V úvodnej kapitole si priblížime niekoľko základných pojmov, ktoré sa týkajú informačnej bezpečnosti. Povieme si, čo predstavuje informačná bezpečnosť v súčasnej informačnej spoločnosti, čo je hlavným cieľom informačnej bezpečnosti a aké metódy a postupy sa v informačnej bezpečnosti najčastejšie využívajú. Definujeme si pojmy ako informačný systém, bezpečnostný útok, bezpečnostné riziko a bezpečnostná hrozba. Zároveň sa pokúsime zhodnotiť, aké miesto zaberá informačná bezpečnosť v kontexte súčasného vzdelávania a výučby informatiky na stredných a stredných odborných školách v SR. Kladieme si za cieľ zmapovať nielen Inovovaný štátny vzdelávací program ISCED-3A určený pre gymnáziá so štvorročnou a päťročnou výukou a Štátny vzdelávací program určený pre stredné školy s odborným vzdelávaním ISCED-3C, ale aj školské vzdelávacie programy niektorých vybraných gymnázií a stredných odborných škôl.

1.1 Úvod do informačnej bezpečnosti

Informácie majú v súčasnej dobe veľkú hodnotu. Sú súčasťou nášho každodenného života a keďže patríme do informačnej spoločnosti, denne informácie posielame, prijímame, vyhodnocujeme či spracovávame. Niektoré informácie sú pre nás nehodnotné, iné naopak, majú nevyčísliteľnú hodnotu. S využitím informácii súvisí aj prudký rozvoj informačno-komunikačných technológií (IKT), ktoré majú veľký podiel na efektívnom spracovaní informácií, avšak takisto otvárajú nové možnosti zneužitia informácií.[1]

1.1.1 Informácie a informačné systémy

Definovanie informácie nie je priamočiare a často závisí od perspektívy, z ktorej informáciu skúmame. Vo všeobecnosti môžeme informáciou označiť ako údaj, resp. súbor údajov, ktorý je nositeľom významu. Hodnota údajov, ktoré tvoria informáciu závisí aj od kontextu, v ktorom sa informácia nachádza. Informácia môže byť reprezentovaná rôznymi spôsobmi, najčastejšie pomocou textu či hovoreného slova. [2] Informácia je teda zaznamenaná pomocou údajov, ktoré majú podobu konečnej postupnosti znakov nad nejakou konečnou abecedou. Potom môžeme samotné údaje chápať ako zápis informácie a naopak, informáciu ako to, čo vyplýva z obsahu údajov.[3]

[1] porov. D. Olejár et all, 2013, s. 11
[2] porov. P. Aksoy, L. Denardis,2007, s. 3-4
[3] porov. D. Olejár et all, 2013, s. 11

Informácie spracovávame pomocou informačných systémov (IS). Informačný systém nie je len samotný hardvér, ktorý zabezpečuje prácu s informáciami. Ide o celú sadu softvéru, hardvéru, dát, ľudí, procedúr a sietí, ktoré umožňujú využitie informačných zdrojov v spoločnosti. Každý z týchto komponentov informačného systému má nielen svoje silné, ale aj slabé stránky, ktoré môžeme označiť za zraniteľnosti. Každý z týchto komponentov má teda aj vlastné požiadavky na bezpečnosť.[4]

Od bezpečného informačného systému sa vyžaduje, aby pracoval s informáciami tak, aby si zachovali svoje hlavné charakteristiky, ktoré udávajú ich hodnotu:[5]

- **Dostupnosť informácie** – informácia musí byť dostupná autorizovanému používateľovi, ktorý má oprávnenie pracovať s informáciou, kedykoľvek, keď o to požiada[6]. Informácia by mala byť používateľovi dostupná v požadovanom formáte. Neautorizovaný používateľ k informácii nemá prístup. Dostupnosť ako vlastnosť informácie vidíme na príklade informačného systému knižnice, kde si čitateľ môže požadovanú knihu vyzdvihnúť v čase otváracích hodín a po preukázaní čitateľského preukazu.[7]
- **Integrita informácie** – informácia musí byť kompletná a konzistentná, každá jej modifikácia musí byť oznámená autorizovanému používateľovi, ktorý má k nej prístup. Ak je informácia modifikovaná bez vedomia autorizovaného používateľa, stráca svoju informačnú hodnotu. Ak oprávnená osoba zistí, že došlo k modifikácii, je potrebné, aby si informáciu ešte raz vyžiadala od jej poskytovateľa.[8]
- **Dôvernosť informácie** – informácia nesmie byť zverená neoprávnenému používateľovi, každý používateľ by mal prejsť procesom preukázania identity. Zaručenie tejto vlastnosti znamená, že informácie sa spracúvajú spôsobom, pri ktorom je vylúčená prítomnosť neoprávnených osôb alebo je informácia zapísaná len v takom formáte, v ktorom ju môže prečítať len oprávnený používateľ.[9]
- **Zodpovednosť informácie** – vlastnosť, ktorá umožňuje evidovať udalosti spojené s bezpečnosťou informácie. Znamená to, že ku každej činnosti informačného

[4] porov. M. Whitman, H. Mattord, 2011, s. 16
[5] porov. R. Janošcová, 2014, s. 9-10
[6] porov. D. Olejár et all, 2013, s. 12
[7] porov. M. Whitman, H. Mattord, 2011, s. 12
[8] porov. D. Olejár et all, 2013, s. 12
[9] porov. D. Olejár et all, 2013, s. 12

systému vieme jednoznačne priradiť entitu, ktorá za túto činnosť zodpovedá.[10] Na základe tejto vlastnosti môžeme spätne vysledovať prípadné zneužitie informácie.

- **Autentickosť informácie** – používateľ môže zistiť identitu informácie. Autentickosť informácie zaručuje, že k príjemcovi bude doručená tá istá informácia, ktorú odoslal odosielateľ. Jedná sa o spojenie integrity informácie s jednoznačnou identifikáciou jej odosielateľa alebo tvorcu. [11] Autentickosť ako vlastnosť informácie vidíme na príklade e-mailovej správy. Príjemca e-mailovej správy je presvedčený o tom, že doručená správa je autentická s tou, ktorú mu odoslal odosielateľ. Ak však útočník zmení obsah e-mailovej komunikácie (e-mail spoofing), nie je možné prijatú správu označiť ako autentickú.[12]
- **Užitočnosť informácie** – informácia musí mať pre používateľa hodnotu, musí vyhovovať účelu, na ktorý si ju používateľ vyžiadal. Na to, aby bola informácia užitočná, musí byť vo formáte, v ktorom ju používateľ vyžadoval. [13]

K spomenutým charakteristikám informácií niektorí autori zaraďujú ešte súkromnosť, či bezpečnostné požiadavky zamerané na komunikáciu ako je nepopretie pôvodu a nepopretie prijatia, anonymitu a pseudonymitu.[14] Z veľkého počtu bezpečnostných útokov vyplýva, že informačná bezpečnosť by sa mala zamerať hlavne na dôvernosť, integritu a dostupnosť informácie.[15]

1.1.2 Definícia informačnej bezpečnosti

Informačná bezpečnosť je multidisciplinárna oblasť, čo znamená, že v sebe sústreďuje poznatky z viacerých disciplín, nielen z informatiky, ale aj zo softvérového inžinierstva, manažmentu, práva či psychológie. Každú túto oblasť však spája spoločný cieľ, a to chrániť dáta a informácie, ktoré majú pre nás hodnotu.[16] Môžeme povedať, že úlohou informačnej bezpečnosti je chrániť dôvernosť, dostupnosť a integritu informačných aktív počas celého procesu ukladania, spracovávania a prenosu. Ide o základné charakteristiky informácie, ktoré sme uviedli v predchádzajúcej podkapitole. Informačnú bezpečnosť aktív môžeme docieliť aplikáciou bezpečnostnej politiky, vzdelávaním oprávnených osôb a zvyšovaním povedomia o informačných technológiách.

[10] porov. D. Olejár et all. 2013, s. 13
[11] porov. D. Olejár et all, 2013, s. 12
[12] porov. M. Whitman, H. Mattord, 2011, s. 12
[13] porov. M. Whitman, H. Mattord, 2011, s. 15
[14] porov. D. Olejár et all. 2013, s. 12-13
[15] porov. T. R. Peltier, 2013, s. 39
[16] porov. R. Janošcová, 2014, s. 7

Informačná bezpečnosť je spolu s fyzickou, personálnou, komunikačnou, operačnou a sieťovou bezpečnosťou dôležitým konceptom organizačnej bezpečnosti.[17] Ich spoločnou úlohou je chrániť aktíva organizácie pred poškodením či zneužitím. V súvislosti s využitím informačnej bezpečnosti v rámci organizácie je dôležité dodržiavať niekoľko pravidiel:[18]

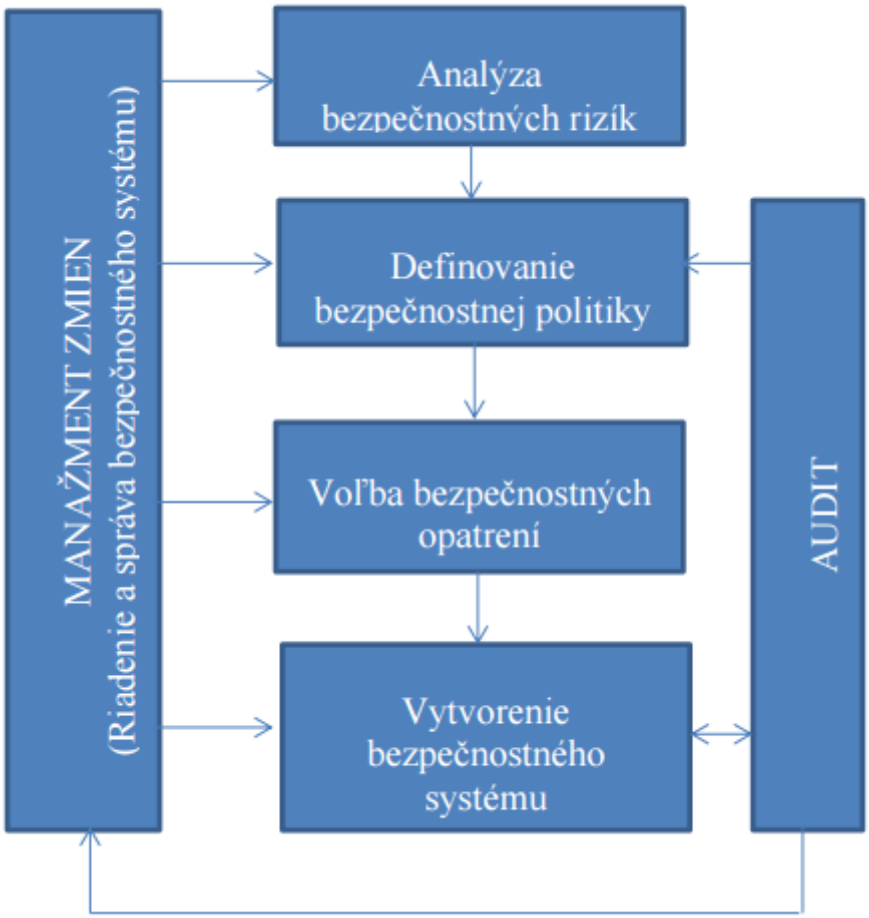
- Informačná bezpečnosť by mala dodržiavať cieľ a poslanie organizácie. Osoby alebo jednotlivé súčasti organizácie by nemali byť informačnou bezpečnosťou zaťažené natoľko, aby negatívne ovplyvnili záujmy organizácie, napríklad vytvárať finančný zisk.
- Riadenie informačnej bezpečnosti je spojené s povinnosťou lojality – všetky rozhodnutia musia byť urobené v najlepšom záujme organizácie, a to zodpovedne a kvalifikovane.
- Informačná bezpečnosť musí byť v rámci organizácie zavedená efektívne. Efektivita informačnej bezpečnosti stojí hlavne na správnom zhodnotení bezpečnostných rizík a hrozieb, ktoré bezprostredne ohrozujú organizáciu.
- Je potrebné explicitne stanoviť osoby v rámci organizácie, ktoré zodpovedajú za informačnú bezpečnosť. Dôležité je primerané rozdelenie rolí medzi všetkých členov organizácie.
- Organizácia, ktorá disponuje informáciami zodpovedá za ich šírenie. Preto je potrebné dohliadať, či osoby, ktoré pracujú s informáciami majú skutočne autorizovaný prístup.
- Na patričnú mieru ochrany informácií je potrebné zaviesť takzvaný životný cyklus, v rámci ktorého sa neustále prehodnocujú pravidlá informačnej bezpečnosti, dochádza k analýze rizík a dopadov, kategorizácii aktív a k zavádzaniu nových bezpečnostných pravidiel.
- Prehodnocovanie informačnej bezpečnosti a jej pravidiel musí prebiehať dynamicky, a to v súlade s meniacimi sa cieľmi či záujmami organizácie.
- Ochrana informácii prebieha v celej organizácii. Ak sa však organizácia nachádza vo viacerých krajinách, je obmedzená právnymi normami, ktoré majú zákonnú platnosť v danej krajine.

[17] porov. M. Whitman, H. Mattord, 2011, s. 8
[18] porov. T. R. Peltier, 2013, s. xiii-xiiv

Informačnú bezpečnosť si nemôžeme predstaviť ako jednorazové technické riešenie, ktoré bude nadčasové a univerzálne. Informačná bezpečnosť predstavuje neustály a dynamický proces odhaľovania bezpečnostných problémov a hľadania efektívnych riešení, ktoré vyhovejú požiadavkám organizácie. Preto je potrebné informačnú bezpečnosť neustále prehodnocovať. Tento proces prehodnocovania môžeme označiť ako *manažment informačnej bezpečnosti*, v literatúre označovaný pod skratkou ISMS (Information security Management System). [19] ISMS pozostáva z niekoľkých fáz[20]:

1. Najskôr prebieha **analýza možných bezpečnostných rizík**, ktorá v sebe zahŕňa identifikáciu aktív a ich klasifikáciu, identifikáciu bezpečnostných hrozieb a stanovenie pravdepodobnosti ich výskytu, identifikáciu slabých prvkov informačného systému a napokon zhodnotenie zbytkových rizík.
2. Potom prebieha **definovanie bezpečnostnej politiky**. Ide o zoznam bezpečnostných pravidiel a odporúčaní, ktoré by mali používatelia s prístupom k informačnému systému a k jeho aktívam nevyhnutne dodržiavať. Ide o vnútorný právny predpis, ktorý je záväzný pre všetkých členov organizácie. Definuje hlavné bezpečnostné ciele organizácie, identifikuje najdôležitejšie aktíva, stanovuje zásady ich ochrany a v neposlednom rade definuje povinnosti členov organizácie vo vzťahu k informačnej bezpečnosti[21].
3. **Voľba bezpečnostných opatrení** prináša bezpečnostné funkcie, procedúry a mechanizmy spoločne vytvárajúce bezpečnostný projekt.
4. Praktická **realizácia** súvisí s vytvorením bezpečného informačného systému po aplikovaní zmien, zlepšení a opráv.
5. **Audit** je fáza opätovného prehodnotenia bezpečnostného systému a bezpečnostnej politiky, ktorá vedie proces bezpečnosti znovu na hranicu definovania bezpečnostnej politiky.

[19] porov. D. Olejár et all. 2013, s. 16
[20] porov. R. Janoščová, 2014, s. 13-14
[21] porov. D. Olejár et all. 2013, s. 17-18



Obr. 1 Životný cyklus informačnej bezpečnosti

1.1.3 Bezpečnostná hrozba, bezpečnostné riziko a zraniteľnosť.

Skôr, ako môžeme zostaviť bezpečnostnú politiku organizácie, musíme poznať bezpečnostné hrozby, riziká a zraniteľnosti, ktoré vyplývajú zo štruktúry organizácie a môžu rôznymi spôsobmi ovplyvniť hodnotu aktív organizácie.

Pod *bezpečnostnou hrozbou* rozumieme kategóriu objektov, osôb alebo iných entít, ktoré predstavujú pre aktíva organizácie potencionálne nebezpečenstvo. [22] Príkladom bezpečnostnej hrozby je neoprávnená osoba, ktorá získa prístupové údaje do informačného systému. V reálnom živote môže byť pre nás bezpečnostnou hrozbou zabudnutý dáždnik, ktorý môže ohroziť naše zdravie v prípade nečakaného dažďa.[23] Bezpečnostná hrozba môže byť riadená alebo neriadená[24]:

[22] porov. M. Whitman, H. Mattord, 2011, s. 11
[23] porov. A. Taylor, 2013, s. 19-20
[24] porov. M. Whitman, H. Mattord, 2011, s. 11

- Príkladom *riadenej bezpečnostnej hrozby* je plánovaný útok na informačný systém s cieľom získať, poškodiť alebo zneužiť jeho informácie. Označuje sa aj ako úmyselná bezpečnostná hrozba.
- *Neriadená bezpečnostná hrozba* je vecou náhody, ako napríklad prípadná prírodná pohroma, ktorá mimovoľne ohrozuje budovy, v ktorých sa nachádza hardwarová časť informačného systému.

Ďalšia kategorizácia rozdeľuje bezpečnostné hrozby na vnútorné a vonkajšie[25]:

- *Vnútorné bezpečnostné hrozby* vznikajú v rámci samotnej organizácie, teda od osôb, ktoré majú určitý stupeň oprávnenia manipulovať s informáciami. Vnútorné bezpečnostné hrozby môžu byť úzko spojené s dodávateľmi či externými spolupracovníkmi organizácie, ale aj so samotnými zamestnancami.
- *Vonkajšie bezpečnostné hrozby* vznikajú mimo organizácie, napríklad v rámci konkurenčného boja.

Bezpečnostná hrozba predstavuje len potenciál na vykonanie zraniteľnosti. Nemusí byť realizovaná, no skutočne nebezpečnou sa stáva v prípade, ak existuje jej reálny vykonávateľ – útočník. Pravdepodobnosť realizácie bezpečnostnej hrozby je dôležitá pri posudzovaní a riadení bezpečnostných rizík informačného systému.[26]

Zraniteľnosť je určitý nedostatok alebo porucha v informačnom systéme alebo v jeho ochrannom mechanizme. Umožňuje uskutočnenie útoku alebo poškodenie uložených dát a informácií v informačnom systéme. Medzi rozšírené zraniteľnosti patrí napríklad nechránený systémový port alebo chyba v programovom vybavení počítača. Najznámejšie zraniteľnosti sú zdokumentované a publikované tak, aby sa informačné mohli dostatočne včas vyhnúť útoku aplikovaním bezpečnostných pravidiel či prípadnou opravou zraniteľnosti.[27] Zraniteľnosti môžeme zaradiť do dvoch kategórii[28]:

- *Univerzálne zraniteľnosti* zahŕňajú základné nedostatky v informačnom systéme, ktoré sa týkajú všetkých jeho súčastí, teda nielen chýb hardvéru a softvéru, ale aj pochybenia ľudí, procesov a postupov.

[25] porov. A. Taylor, 2013, s. 20
[26] porov. S. Elky, 2006, s. 15
[27] porov. M. Whitman, H. Mattord, 2011, s. 11
[28] porov. A. Taylor, 2013, s. 20-21

- *Informačne špecifické zraniteľnosti* sa týkajú hlavne nezabezpečených informačných systémov, či už osobných počítačov, pamäťových kariet alebo USB zariadení, nezabezpečených sieťových pripojení či webových serverov.

Bezpečnostné riziko predstavuje pravdepodobnosť poškodenia aktíva, ktorá vyplýva buď z prebiehajúceho procesu, alebo z existujúcej udalosti. Z hľadiska informačnej bezpečnosti je *manažment rizík* proces porozumenia a následnej reakcie na faktory, ktoré môžu viesť k poškodeniu integrity, dostupnosti a dôvernosti informácie a informačného systému. Príkladom zvyšujúceho sa bezpečnostného rizika je informačný systém s neošetrenými zraniteľnosťami, ktorý tak ohrozuje informácie v ňom spracovávane. [29] Manažment rizík pozostáva zo štyroch fáz[30]:

- *Identifikácia hrozieb* súvisí s pravidelnou kontrolou zraniteľností informačného systému. Úlohou prvej fázy je včasná identifikácia možného ohrozenia informačného systému. Vhodné je vytvoriť zoznam aktív, ktoré sú pre informačný systém kritické, a potom sledovať potencionálne ohrozenia týchto aktív. Nové typy bezpečnostných hrozieb neustále vznikajú, preto je potrebné pravidelne dbať na ich identifikáciu. Každú nájdenú hrozbu je potrebné posudzovať v kontexte jej dopadu na aktívum.
- *Analýza vplyvu* identifikovaných hrozieb a *hodnotenie ich dopadu* pre organizáciu predstavujú druhú fázu cyklu riadenia rizík. Potom, ako zhodnotíme možný vplyv každej bezpečnostnej hrozby, posúdime aj pravdepodobnosť jej možného výskytu. Výstupom analýzy a hodnotenia hrozieb je napríklad matica bezpečnostných rizík, ktorá nám umožní kategorizáciu bezpečnostných hrozieb od najprioritnejšej po najmenej závažnú. Takáto matica nám pomôže definovať rôzne úrovne rizík v rámci organizácii a je taktiež východiskom pre stanovenie rizikovej tolerancie. Najvyššia miera dopadu a pravdepodobnosti vzniku spôsobuje nárast kritickosti bezpečnostnej hrozby. Takáto hrozba by sa v rámci bezpečnostnej politiky mala riešiť čo možno najurgentnejšie.
- *Ošetrenie rizík* sa uskutočňuje zvolením jedného z nasledujúcich postupov:

[29] porov. S. Elky, 2006, s. 1
[30] porov. A. Taylor, 2013, s. 24-28

- *Vyhnúť sa bezpečnostnému riziku* ukončením procesu, ktorý ho spôsobuje. Príkladom je zavedenie pravidla do bezpečnostnej politiky, ktoré hovorí o zákaze používania neautorizovaného softvéru.
- *Akceptovať bezpečnostné riziko* v prípade, ak je jeho úroveň v hodnotení rizík posudzovaná ako nízka. Tolerancia rizika neznamená jeho ignorovanie. O akceptácii rizika by mali byť informovaní všetci členovia organizácie. Príkladom akceptovaného rizika je riziko, pri ktorom náklady na jeho odstránenie prekročia potencionálny finančný dosah škôd, ktoré by mohlo spôsobiť. Aj akceptované riziká sú neustále monitorované, a to preto, aby sme mohli predísť prípadnému neželanému prehodnoteniu rizika na riziko s vysokou prioritou.
- *Znížiť alebo upraviť bezpečnostné riziko* môžeme tromi spôsobmi, a to redukciou bezpečnostnej hrozby, zraniteľnosti a napokon redukciou dopadu rizika. Napríklad aplikovaním vhodných bezpečnostných záplat či dôkladným nastavením firewallu znížime pravdepodobnosť ukradnutia prístupových údajov, ale úplne sa takémuto útoku nevyhneme. Eliminovať možné škody môžeme taktiež uložením informačných aktív organizácie do viacerých informačných systémov. V prípade zlyhania jedného z nich sa tak môžeme spoľahnúť na zálohu informačných aktív uloženú v nenapadnutých informačných systémoch.
- *Zdieľanie alebo prenos bezpečnostného rizika* znamená prenesenie zodpovednosti za jeho realizáciu na inú organizáciu, ktorá sa buď zaoberá odborným manažmentom rizík alebo poskytuje poistenie v prípade realizácie bezpečnostnej hrozby.

- *Monitorovanie* môžeme označiť ako konečnú fázu cyklu riadenia rizík. Cieľom tejto fázy je pravidelná kontrola bezpečnostných hrozieb a prehodnocovanie rizika ich realizácie. Ide o dynamický proces, keďže niektoré hrozby môžu zaniknúť, rovnako však môžu vzniknúť nové, dosiaľ nepoznané hrozby. Prostredníctvom monitorovania dokážeme overiť funkcionalitu a efektívnosť ošetrenia bezpečnostných rizík.

1.2 Informačná bezpečnosť v kontexte vyučovania informatiky

Kurikulum sa v pedagogickej praxi považuje za súbor dokumentov, ktorých úlohou je komplexne definovať zámery vyučovacieho procesu. Neoddeliteľnou súčasťou kurikula sú informácie o učebných cieľoch, o obsahu učiva, bližšie sa špecifikujú vyučovacie a študijné metódy, prostriedky a postupy. Kurikulum nepredstavuje však len obsahovú náplň vyučovania, ale aj dosiahnutú skúsenosť žiakov, ktorá je výsledkom vyučovacieho procesu. Do kurikula patria oficiálne dokumenty ako Štátny vzdelávací program (ŠVP), ale aj dokumenty, ktoré si škola prípadne učiteľ vytvára sám, na základe vlastných skúseností so žiakmi. Prostredníctvom kurikula si vieme zodpovedať na základné otázky, ktoré sa týkajú učiva, a síce prečo, čo, kedy, ako, za akých podmienok a s akým očakávaným výsledkom máme vyučovať. [31] V tejto podkapitole budeme analyzovať informačnú bezpečnosť z pohľadu oficiálneho kurikulárneho vzdelávania na gymnáziách a stredných odborných školách v Slovenskej republike.

1.2.1 Štátny vzdelávací program

Štátny vzdelávací program je dokument, ktorý je záväzný pre vzdelávacie inštitúcie na území Slovenskej republiky. Od roku 2015 vstúpil do platnosti Inovovaný štátny vzdelávací program (IŠVP), ktorý ponúka učebné ciele definované prostredníctvom obsahových a výkonnostných štandardov. Pre vyučovanie informatiky na gymnáziách so štvorročným a päťročným vzdelávacím programom sa stáva záväzným Inovovaný štátny vzdelávací program ISCED-3A, ktorý je členený do piatich oblastí, a *to Reprezentácia a nástroje, Komunikácia a spolupráca, Algoritmické členenie problémov, Softvér a hardvér* a *Informačná spoločnosť*.[32] Informačná bezpečnosť je čiastočne zaradená v oblasti *Informačná spoločnosť-bezpečnosť a riziká*, kde sa následne pre žiakov definujú výkonové a obsahové štandardy:

Tab. 1 Oblasť IŠVP Informačná spoločnosť - bezpečnosť a riziká[33]

Výkonový štandard	Obsahový štandard
Žiak vie/ dokáže ✓ posudzovať riziká práce na počítači so škodlivým softvérom,	*Procesy:* šírenie počítačových vírusov a spamov, bezpečné a etické správanie sa na

[31] porov. I. Turek, 2008, s. 196 - 197
[32] porov. Štátny pedagogický ústav, 2015, s. 1
[33] Štátny pedagogický ústav, 2015, s. 17

✓ aplikovať pravidlá pre zabezpečenie prístupu do e-mailu, do komunity, do počítača a proti neoprávnenému použitiu, ✓ zabezpečiť svoje údaje a komunikáciu proti zneužívaniu, ✓ hodnotiť dôvernosť informácií na webe, ✓ rozpoznávať počítačovú kriminalitu, ✓ rozlišovať nelegálny obsah	internete, činnosť hekerov, nezverejňovanie vlastných údajov na internete.

V oblasti *Hardvér a softvér* nájdeme nasledujúce štandardy týkajúce sa informačnej bezpečnosti:

Tab. 2 Oblasť IŠVP Hardvér a softvér - práca proti vírusom a špehovaniu[34]

Výkonový štandard	Obsahový štandard
Žiak vie/ dokáže ✓ využívať nástroje na odhaľovanie a odstraňovanie škodlivého softvéru.	*Vlastnosti a vzťahy*: vírus ako škodlivý softvér, špehovanie ako nepovolená aktivita softvéru alebo webových stránok, antivírus ako softvér na zisťovanie a odstraňovanie škodlivého softvéru a blokovanie škodlivých činností, obmedzenia antivírusových programov (antivírus je tiež iba program, a nemusí odhaliť najnovší bezpečnostný softvér)

Inovovaný štátny vzdelávací program ponúka učivo štruktúrované do tematických celkov, ktoré predstavujú obsahový štandard predmetu Informatika. Obsahový štandard si môžu učitelia tvorivo modifikovať v závislosti od schopností žiakov, dôležité však je, aby bol naplnený celý vzdelávací štandard.[35]

[34] Štátny pedagogický ústav, 2015, s. 16
[35] Štátny pedagogický ústav, 2015, s. 1

Štátny vzdelávací program pre stredné odborné školy vytvára Štátny inštitút odborného vzdelávania, a to v závislosti od zvoleného typu študijného odboru či dĺžky štúdia absolventa. V našej práci sme sa zamerali na analýzu výuky informačnej bezpečnosti v študijnom odbore *Mechanik počítačových sietí*, ktorý má blízko k informačným systémom a k samotnej informačnej bezpečnosti. Pre spomenutý študijný odbor je platný *Štátny vzdelávací program ISCED-3C – Elektrotechnika 26*, ktorý bol schválený Ministerstvom školstva v roku 2013 a následne modifikovaný dodatkami, ktoré vstúpili do platnosti v rokoch 2013 a 2015. Spomenutý posledný dodatok prináša pre stredné odborné školy tohto zamerania vzorové učebné osnovy odborných predmetov. Spomedzi siedmych odborných predmetov (elektrotechnika, technické vybavenie počítačov, programové vybavenie počítačov, elektronika, elektrické merania, elektrotechnická spôsobilosť a ekonomika) sa informačná bezpečnosť vyučuje v rámci predmetu Technické vybavenie počítačov.[36] Vzorová učebná osnova tohto predmetu prináša nasledujúce témy, ktoré súvisia s informačnou bezpečnosťou:

Tab. 3 Informačná bezpečnosť v rámci vzorových učebných osnov ŠVP [37]

Odborný predmet	Názov tematického celku	Téma/ Učivo	Ročník
Technické vybavenie počítačov	Bezdrôtové siete WiFi	Bezpečnosť WLAN sietí	4.
	Bezpečnosť – VPN siete	Charakteristika a typy VPN sietí, GRE tunel, IPsec	
	Bezpečnosť sietí	Firewall	
		Opatrenia na zabezpečenie sietí	
		Symetrické a asymetrické šifrovanie	
		Analýza sieťovej prevádzky a sv. prostriedky	

[36] Štátny inštitút odborného vzdelávania, 2015, s. 76 - 106
[37] Štátny inštitút odborného vzdelávania, 2015, s. 83 - 88

1.2.2 Školský vzdelávací program

Ďalším dôležitým oficiálnym dokumentom kurikula je Školský vzdelávací program (ŠkVP), ktorý si stanovuje škola samostatne, a to na základe aktuálneho a prislúchajúceho Štátneho vzdelávacieho programu. Školský vzdelávací program je často zverejnený na webovej stránke školy. Jeho úlohou je definovať ciele výchovy a vzdelávania na vybranej škole, predstavuje nám profil absolventa školy, zameranie školy, ale aj učebné plány, osnovy a učebné zdroje, ktoré sú taktiež súčasťou kurikula. Vychádzajúc zo ŠkVP vybraných stredných škôl Košického a Prešovského kraja sme vytvorili prehľadnú tabuľku učebných tém predmetu Informatika súvisiacich s vyučovaním informačnej bezpečnosti na stredných školách:

Tab. 4 Témy informačnej bezpečnosti obsiahnuté v predmete Informatika [38]

Názov školy	**Typ školy**	**Ročník**	**Téma (kompetencie)**	
Gymnázium Poštová	Gymnázium	2.	Bezpečnosť na Internete, ochrana počítača.	
			Ochrana používateľa počítača.	
			Šifrovanie a hashovanie.	
Gymnázium Opatovská	Gymnázium	3.	Bezpečnosť na Internete	*Poznať spôsoby ochrany počítača zapojeného v sieti a osoby na ňom pracujúcej.*
Gymnázium Jána Adama Raymana	Gymnázium	3.	Riziká informačných technológií	*Malware – základné pojmy, detegovanie a prevencia. Kriminalita.*
			Etika a právo	*Autorské práva na softvér, licencia (freware, shareware, multilicencia, demo verzia, Open source)*

[38] Štátny inštitút odborného vzdelávania, 2015, s. 83 - 88

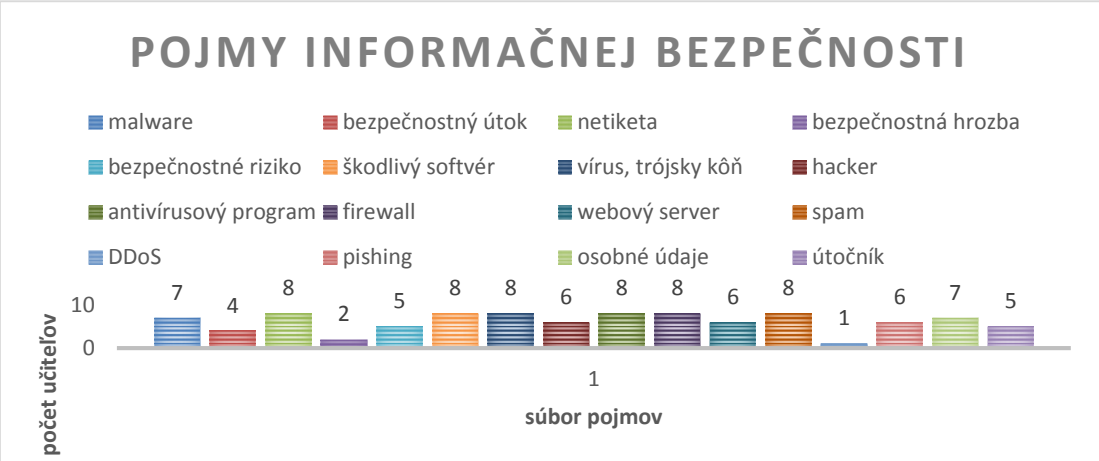
1.2.3 Skúsenosti učiteľov s výučbou informačnej bezpečnosti

V rámci realizácie Klubu učiteľov informatiky s témou *Aspekty bezpečnosti vo vyučovaní informatiky* sme mali možnosť opýtať sa učiteľov základných a stredných škôl na mieru začlenenia výučby informačnej bezpečnosti do predmetu Informatika v pedagogickej praxi. Na položené otázky nám odpovedali ôsmi učitelia pôsobiaci na základných školách, gymnáziách a osemročných gymnáziách. Anketa, formou ktorej sme zisťovali odpovede je k dispozícii v prílohe s názvom *Dotazník k výučbe informačnej bezpečnosti*.

V jednej z otázok sme poskytli učiteľom súbor pojmov týkajúcich sa informačnej bezpečnosti. Učitelia z nich označili tie, ktoré sú súčasťou výučby informatiky na škole, v ktorej pôsobia a vyučujú. Uvedený graf zobrazuje počet vyučujúcich, ktorí aplikujú vybrané pojmy do obsahu učiva. Medzi najrozšírenejšie pojmy informačnej bezpečnosti, ktoré sú súčasťou výučby informatiky patrí malvér, netiketa, škodlivý softvér, vírus, trójsky kôň, antivírusový program, firewall či spam.

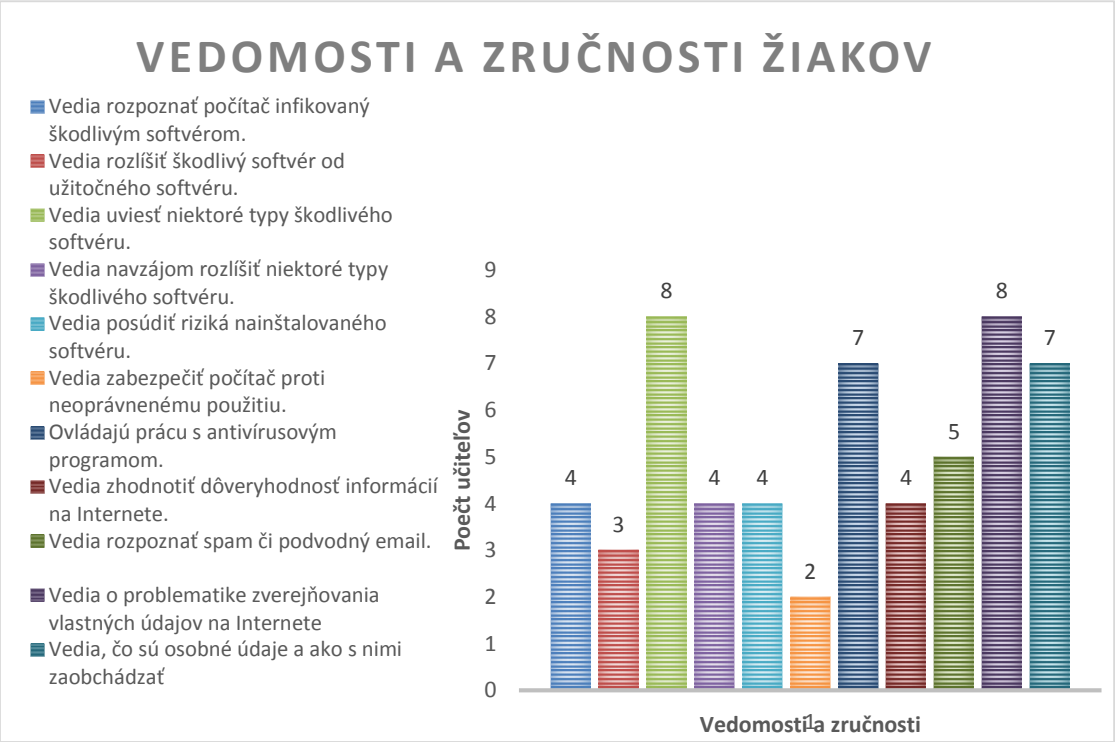
Naopak, z odpovedí vyplýva, že študenti sa často nestretnú s pojmami ako bezpečnostná hrozba a bezpečnostné riziko. Na chvoste výučby stojí pojem DDos útok (Distributed Denial of Service), ktorý je zrejme pre mnohých študentov náročný na pochopenie a presahuje základné učivo.

Graf. 1 Pojmy informačnej bezpečnosti vo výučbe informatiky



Ďalšia otázka ankety o výučbe informačnej bezpečnosti bola venovaná vedomostiam a zručnostiam študentov, ktoré študenti podľa učiteľov ovládajú po úspešnom absolvovaní predmetu Informatika. Tvrdenia, ktoré korešpondujú s náplňou ich vyučovacích hodín učiteľov sú zobrazené na grafe č. 2 nasledovne:

Graf. 2 Vedomosti a zručnosti žiakov z informačnej bezpečnosti



Z uvedeného grafu môžeme vyčítať, že študenti väčšinou ovládajú prácu s antivírusovým systémom a dokonca vedia uviesť niektoré typy škodlivého softvéru. Problematické je posudzovanie bezpečnostných rizík nainštalovaných programov či súborov stiahnutých z Internetu.

Rozsah vedomostí žiakov samozrejme závisí aj od počtu vyučovacích hodín, ktoré sú venované vyučovaniu informačnej bezpečnosti. Učitelia základných škôl venujú informačnej bezpečnosti dve hodiny v rámci školského roka, zatiaľ čo učitelia stredných škôl a osemročných gymnázií venujú tejto problematike v priemerne štyri vyučovacie hodiny. Šiesti z opýtaných učiteľov sa vyjadrili, že by privítali navýšenie počtu hodín predmetu Informatika s cieľom rozšíriť vedomosti žiakov o poznatky z informačnej bezpečnosti. Mnohí z nich preto poukazujú na potrebu vytvorenia metodického materiálnu na výučbu informačnej bezpečnosti, či vytvorenia rôznych didaktických pomôcok ako plagátov, webovej stránky či konkrétnych praktických ukážok, ktoré by potom mohli predstaviť svojím žiakom.

2 Honeypot ako pomôcka pri výučbe informačnej bezpečnosti

V rámci tejto práce sme sa rozhodli použiť honeypoty ako didaktický prostriedok na výučbu informačnej bezpečnosti. Preto je dôležité ozrejmiť ich spôsob fungovania a úlohu v informačnej bezpečnosti pri ochrane informácií a informačných systémov. V tejto kapitole sa budeme venovať definícii honeypotu ako počítačového systému, kategorizujeme honeypoty podľa rôznych charakteristík a spôsobov využitia. Zároveň si priblížime už realizované projekty na zahraničných univerzitách, v rámci ktorých bol honeypot použitý ako didaktický prostriedok. Na záver zhodnotíme využitie honeypotu v rámci zážitkového vyučovania.

2.1 Definícia a využitie honeypotov

Najväčšou výzvou každej organizácie zaoberajúcej sa informačnou bezpečnosťou je spoznať potencionálneho útočníka skôr, ako skutočne zaútočí na informačný systém. Okrem spoznania identity útočníka je vhodné zamerať sa aj na spôsob útočenia, teda aké postupy útočník používa, v aký čas sa rozhodne vykonať útok, ako nakladá s informáciami, ktoré by získal v prípade útoku. Získané informácie o útočníkovi tak pomôžu nielen odhaliť motiváciu útočníka, ale aj predísť samotnému bezpečnostnému útoku. Honeypoty sú schopné zaznamenať tieto informácie a pomôcť tak k vyriešeniu závažných otázok informačnej bezpečnosti. [39]

Honeypot môžeme definovať ako počítačový systém, ktorý bol nasadený za účelom podrobného sledovania a študovania bezpečnostných útokov, pre ktorých je ľahkým cieľom. [40] Azda najznámejšiu definíciu honeypotu podáva *L. Spitzner* vo svojej knihe *Honeypots: Tracking Hackers*. Uvádza, že ide o ***bezpečnostný zdroj, ktorého hodnota spočíva v tom, že je sledovaný, napadnutý alebo ohrozený***. Pod takýmto zdrojom si nemusíme vždy predstavovať konkrétny počítač či operačný systém, môže ísť aj o smerovač zapojený do siete, skript simulujúci určitú sieťovú službu alebo produkčný systém.[41]

Honeypot je skutočne ľahký cieľ pre útočníkov – je tomu tak preto, že v rámci počítačovej siete vystupuje ako zariadenie, ktoré má veľký počet nezabezpečených zraniteľností a nedostatkov. Vo chvíli, keď útočník zaútočí na honeypot, stáva sa sám obeťou – honeypot zaznamená každý jeho krok, či už ide o súbory, ktoré útočník otvára a modifikuje, pokusy o prihlásenie sa na vzdialený server, alebo spúšťanie konkrétnych príkazov. Niektoré

[39] porov. Joshi R.C., Anjali S., 2011, s. 2
[40] porov. Spitzner, 2003, s. 15-23
[41] porov. Spitzner, 2003, Honeypots: Tracking Hackers, s. 58

honeypoty dokážu simulovať celý operačný systém, iné sú zamerané na prevádzku konkrétnych sieťových služieb.[42] Úlohou honeypotu je napodobniť produkčný systém vo svojom správaní čo možno najpresnejšie, aby útočník zhodnotil honeypot ako informačný systém vhodný na uskutočnenie útoku. Informačné zdroje, ktorými disponuje honeypot však nie sú reálne, ich zneužitie preto nemôže poškodiť informačné systémy, ktoré sú v sieti skutočne hodnotné.[43]

V rámci počítačovej siete sa môžu vyskytovať viaceré honeypoty. Ak ide o riadenú sieť honeypotov, označujeme ju ako ***honeynet.*** Zvyšovaním počtu honeypotov v honeynete môžu súčasne narastať aj požiadavky na bezpečnosť počítačovej siete. Výhoda honeynetov však spočíva v tom, že dokážu zaznamenať väčšie množstvo dát a tým aj viac informácii o útočníkovi. [44]

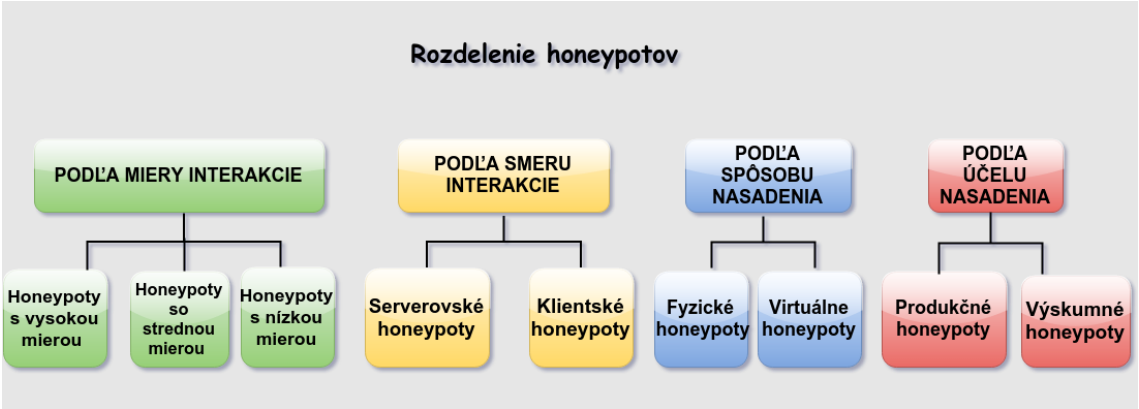
2.2 Kategorizácia honeypotov

Skôr, ako si zvolíme jeden z honeypotov ako didaktickú pomôcku a začleníme ho do vytvoreného laboratória informačnej bezpečnosti, mali by sme vedieť zodpovedať na nasledujúce otázky[45]:

- Aký je hlavný dôvod inštalácie honeypotu do počítačovej siete?
- Ako vyzerá prostredie, počítačová sieť alebo operačný systém, ktorého bude honeypot súčasťou?
- Aký server alebo službu má emulovať honeypot?
- Aký typ bezpečnostných hrozieb (vonkajšie, vnútorné) bude honeypot monitorovať?
- Čo bude ponúkanou návnadou pre útočníka (nezabezpečený systém, alebo systém s klasickou ochranou používanou v bežných podmienkach)?

V súvislosti s uvedenými otázkami sa v literatúre vyskytujú rozdelenia honeypotov do viacerých skupín, a to podľa miery interakcie honeypotu a útočníka, podľa spôsobu nasadenia, podľa smerovania interakcie, ktoré definuje aktivitu honeypotu pri komunikácii s útočníkom a v neposlednom rade rozdeľujeme honeypoty podľa účelu použitia. Nasledujúci obrázok bližšie popisuje rozdelenie honeypotov podľa spomenutých kritérií:

[42] porov. Joshi R.C., Anjali S., 2011, s. 7-8
[43] porov. Gorzelak, K., et al, 2012, s. 17
[44] porov. Spitzner, 2003, Honeypots: Tracking Hackers, s. 99
[45] porov. Joshi R.C., Anjali S., 2011, s. 15



Obr. 2 Kategorizácia honeypotov

2.2.1 Rozdelenie honeypotov podľa miery interakcie s útočníkom

Jednotlivé honeypoty sa navzájom líšia aj tým, do akej miery komunikujú s útočníkom. Podľa toho delíme honeypoty na honeypoty *s nízkou, strednou a vysokou mierou interakcie*. Môžeme predpokladať, že so stúpajúcou mierou interakcie sa súčasne stupňuje aj riziko, že útočník na základe interakcie rozpozná honeypot a prestane s ním komunikovať.

Honeypoty s nízkou mierou interakcie sú nástroje, ktoré najčastejšie emulujú konkrétne služby alebo klientske aplikácie. Emulácia v tomto kontexte znamená, že honeypot napodobňuje danú službu len čiastočne, s limitovanou funkcionalitou. [46] Tieto honeypoty sú nenáročné na inštaláciu a spravovanie, avšak môžu získať len obmedzené množstvo informácií o útočníkovi. Keďže sú spustené na vyššej vrstve operačného systému, útočník nevie spôsobiť veľké škody, jedine zastaviť emuláciu honeypotu. Honeypoty s nízkou mierou interakcie sa využívajú napríklad na identifikáciu IP adresy útočníka. Medzi takéto honeypoty radíme honeypot *Honeyd* alebo honeypot *Glastopf*. [47]

Honeypoty so strednou mierou interakcie kombinujú užitočné vlastnosti honeypotov s nízkou mierou a s vysokou mierou interakcie. Majú vrstvu virtualizácie, vďaka ktorej dokážu útočníkovi odpovedať očakávané odpovede. Príkaz, ktorý útočník odošle na honeypot je dôsledne analyzovaný, na základe analýzy sa vytvorí odpoveď, ktorú bude útočník považovať za korektnú. Sú náročnejšie ako honeypoty s nízkou mierou interakcie, ich nasadenie vyžaduje dobrú znalosť sieťových protokolov. So stúpajúcou interakciou sa samozrejme aj zvyšuje

[46] porov. Gorzelak, K., et al, 2012, s. 18
[47] porov. Joshi R.C., Anjali S., 2011, s. 15 – 16.

riziko.[48] K honeypotom so strednou mierou interakcie patrí napríklad honeypot *Kippo*, ktorý emuluje činnosť SSH servera.

Honeypoty s vysokou mierou interakcie poskytujú veľké množstvo informácií o útočníkovi, sú však časovo náročné na údržbu a ich prevádzkovanie predstavuje značné riziko. Útočníkovi umožňujú prístup k reálnemu operačnému systému, ktorý nemá takmer žiadne obmedzenia a útočník s ním môže plne komunikovať. Takéto honeypoty sú často umiestnené v dôsledne monitorovanom a riadenom prostredí, zabezpečené firewallom alebo IDS systémom. Samotný honeypot v tomto prípade nemá schopnosť kontrolovať útočníka, to je úlohou sieťových zariadení, v mnohých prípadoch firewallu, ktorý bráni útočníkovi prostredníctvom honeypotu útočiť na iné zariadenia. [49] Tieto honeypoty sa často požívajú ako nástroje pri objavovaní a skúmaní exploitov, zraniteľností, ktoré dosiaľ neboli zdokumentované.

Niektoré honeypoty súčasne kombinujú viaceré levely interakcie, označujú sa ako *hybridné honeypoty*. Najčastejšie ide o kombináciu nízkej a vysokej interakcie, zvolený level interakcie závisí od typu samotného útoku, prípadne konfigurácie honeypotu. Príkladom honeypotu s hybridnou interakciou je honeypot *HoneySpider*, ktorý prostredníctvom nízkeho levelu interakcie filtruje bezpečné a nebezpečné webové stránky, zatiaľ čo stránky, označené predchádzajúcim výberom ako nebezpečné ďalej analyzuje prístupom s vysokou mierou interakcie. [50]

2.2.2 Rozdelenie honeypotov podľa spôsobu nasadenia

Honeypoty môžu byť v rámci počítačovej siete nasadené ako fyzické zariadenia alebo prostredníctvom virtualizácie. Na základe toho ich rozdeľujeme na fyzické a virtuálne honeypoty.

Pod fyzickým honeypotom si môžeme predstaviť skutočné zariadenie s operačným systémom, ktoré je zapojené do počítačovej siete a v rámci nej identifikované svojou IP adresou, prípadne môže poskytovať niektoré typy sieťových služieb. Pojem fyzický honeypot sa často spája s honeypotmi s vysokou mierou interakcie, keďže útočníkovi poskytujeme reálny počítačový systém. Je náročný na praktické využitie a samotnú údržbu, ktorá predstavuje

[48] porov. Joshi R.C., Anjali S., 2011, s. 16.
[49] porov. Spitzner, 2003, Honeypots: Tracking Hackers, s. 96
[50] porov. Gorzelak, K., et al, 2012, s. 19 - 20

navrátenie honeypotu do pôvodného stavu pred útokom. Preto v reálnom produkčnom prostredí fyzický honeypot nemá uplatnenie a využíva sa skôr na výskumné účely.[51]

Virtuálny honeypot má oproti fyzickému honeypotu viacero výhod. Vďaka virtualizácii môžeme umiestniť viacero virtuálnych honeypotov na jediné fyzické zariadenie. Virtualizáciu zabezpečuje virtualizačný softvér (*VMware, VirtualBox*), ktorý umožňuje spustiť viacero virtuálnych honeypotov súčasne. Virtuálne honeypoty nie sú náročné na údržbu, majú nižšie fyzické požiadavky a sú škálovateľné.[52]

2.2.3 Rozdelenie honeypotov podľa smeru interakcie

Smer interakcie rozdeľuje honeypoty na dva základné typy – honeypot, ktorý v komunikácii s útočníkom vystupuje ako *server* a honeypot, ktorý vystupuje ako *klient*.

Honeypot typu server je pasívny, je navrhnutý tak, aby neinicializoval komunikáciu s útočníkom. Je užitočný pri odhaľovaní nových typov bezpečnostných hrozieb, zachytáva malvér a podieľa sa na jeho podrobnej analýze. V tejto kategórii nájdeme honeypoty s nízkou mierou interakcie, ktoré majú v rámci počítačovej siete otvorené značné množstvo portov, čo je samozrejme atraktívne pre útočníka, ktorý práve skenuje rôzne počítačové siete a vyhľadáva potencionálne obete útokov.[53]

Klientsky typ honeypotu je naopak iniciátor komunikácie s útočníkom. Jeho cieľom je vypátrať útočníkov, ktorí využívajú zraniteľnosti konkrétnych produkčných serverov a útočia na zariadenia v sieti.[54] Klientske honeypoty sú často orientované na webové aplikácie, detegujú útoky šírené prostredníctvom webových stránok. Príkladom takého to typu honeypotu je aj *Strider Honeymonkey*, ktorý vyhľadáva a analyzuje webové stránky obsahujúce nebezpečný malvér.

2.2.4 Rozdelenie honeypotov podľa účelu použitia

Honeypoty podľa účelu použitia v rámci počítačovej siete rozdeľujeme na produkčné a výskumné honeypoty.

Produkčné honeypoty sa používajú v produkčnom prostredí, preto je potrebné aby ich nasadenie predstavovalo pre počítačovú sieť a samotné produkčné systémy minimálne riziko.

[51] porov. Joshi R.C., Anjali S., 2011, s. 19.
[52] porov. Provos N., Holz T., 2007, s. 41-42
[53] porov. Gorzelak, K., et al, 2012, s. 18.
[54] porov. Joshi R.C., Anjali S., 2011, s. 19.

Hlavný dôvod pre ich použitie je hlavne minimalizácia bezpečnostných rizík, nie sú natoľko náročné na nasadenie a udržiavanie ako výskumné honeypoty. Na druhej strane však poskytnú menej informácií o útočníkovi, nezameriavajú sa na podrobnú analýzu nástrojov, ktoré útočník používa. V rámci produkčnej siete majú dôležitú úlohu – dokážu včas detegovať pokusy o napadnutie siete a tak upozorniť na jej bezpečnostné zraniteľnosti. V konečnom dôsledku teda znižujú riziko prieniku útočníka do produkčného systému.

Výskumné honeypoty nemajú význam pre produkčnú sieť, používajú sa na zhromažďovanie informácií o bezpečnostných hrozbách, aj tých, ktoré doposiaľ neboli objavené. Často sú súčasťou výskumu bezpečnostných hrozieb. Umožňujú nám dôkladne analyzovať činnosť útočníka, stanoviť líniu útoku, odhaliť motív útočníka. Sú užitočné pri forenznej analýze útoku, keďže dokážu zachytiť rozsiahle množstvo dát o útočníkovi.[55]

2.3 Výhody a nevýhody použitia honeypotov

Použitie honeypotov má v rámci konceptu informačnej bezpečnosti celú radu výhod, napríklad [56]:

- **Zber primeraného množstva dát** – honeypoty síce zbierajú len určitý typ dát o neautorizovaných aktivitách útočníkov, no všetky tieto dáta sú pre organizáciu informačnej bezpečnosti dôležité. Akékoľvek nadviazanie spojenia s honeypotom predpokladá aktivitu útočníka. Namiesto detailného skúmania logovacích záznamov sa teda môžeme zamerať priamo na záznamy, ktorými disponuje honeypot.[57]
- **Minimalizácia počtu falošných poplachov** – takmer všetko, čo honeypot zachytí je útok alebo neoprávnená činnosť, ktorú je potrebné ďalej analyzovať.
- **Nízke náklady na prevádzku a jednoduchosť** – honeypoty nepotrebujú veľké zdroje na to, aby úspešne zachytili činnosť útočníka. Aj napriek jednoduchosti dokážu zaznamenať veľký počet informácií o útočníkovi, sú flexibilné, teda je možné implementovať ich do rôznych prostredí či sieťových architektúr.
- **Šifrovanie** – honeypoty dokážu zachytiť aj šifrované útoky.
- **Využitie IPv6 protokolu** – v súčasnosti honeypoty pracujú aj s IPv6 protokolom.

[55] porov. Mokube I., Adams, M., 2007, s. 322
[56] porov. Spitzner, 2003, s. 18
[57] porov. Kambow, N., Passi, L. K., 2014, s. 6100

- **Objavovanie nových nástrojov a taktík útočníkov** – honeypoty pozitívne prispievajú k objavovaniu nových bezpečnostných zraniteľností a bezpečnostných hrozieb.

Okrem výhod sú známe aj niektoré nevýhody honeypotov: [58]

- **Obmedzený rozhľad** – honeypot monitoruje konkrétnu sieťovú prevádzku, ktorej je sám súčasťou. Ak je sieťová prevádzka nízka, honeypot dokáže odhaliť len nízky počet útočníkov.
- **Priehľadnosť** – v niektorých prípadoch je honeypot pre útočníka ľahko rozpoznateľný. Ak je honeypot rozpoznaný útočníkom, predstavuje pre sieť ďalšie riziko. V závislosti od kategórie honeypotu sa rozlišuje aj miera rizika, najvyššie riziko predstavujú honeypoty s vysokou mierou interakcie.
- **Riziko prevzatia** – prostredníctvom honeypotu môže byť uskutočnený útok aj na iné informačné systémy.
- **Zlé rozhodnutia** – používanie honeypotu môže niekedy viesť k zlým rozhodnutiam v rámci bezpečnostnej politiky počítačovej siete.

2.4 Honeypot ako edukačná pomôcka

Vzdelávanie je v informačnej bezpečnosti veľmi dôležité, či už na strane laikov alebo odborníkov v sieťových technológiách. V rámci didaktických koncepcii sa hovorí o konštruktivizme, ktorý si zakladá na koncepcii konštruovania vedomostí na základe vzájomnej interakcie s okolím. Študent si sám vytvára vlastný konštrukt vedomostí, pričom nové vedomosti by mali nadväzovať prípadne pretvárať vedomostný konštrukt, s ktorým študent disponuje. Dôležité je pri tom zážitkové vnímanie nových poznatkov, ktoré sa tak rýchlejšie zapíšu do vedomostného konštruktu študenta. [59]

Honeypoty môžeme pri výučbe informačnej bezpečnosti chápať ako generatívno-inštruktážne didaktické prostriedky, ktoré poskytujú určité pokročilé ukážky interaktívnych prvkov, čo umožňuje vysokú úroveň praktickej skúsenosti pre študenta.[60] Vďaka honeypotom si študenti môžu vyskúšať rôzne bezpečnostné incidenty, s ktorými sa môžu stretnúť v reálnej prevádzke alebo pri konfigurácií počítačových sietí. Honeypot nám môže poslúžiť aj ako

[58] Adeel, M., et al., 2005, s. 1-6
[59] TUREK, I., 2008, s. 397 - 398
[60] López, M. H., Reséndes, C. F., 2008, s. 73- 74

užitočná pomôcka pri viacerých prierezových témach, ako je napríklad nastavovanie softvéru a hardvéru, práca s rôznymi sieťovými službami, ktoré sa používajú v rámci servera, práca s logmi operačného systému, sieťové nastavenia, práca s nainštalovanými aplikáciami, manažovanie operačného systému a získavanie základných informácií o nastaveniach informačného systému ako takého.[61]

V rámci pedagogickej praxe sa už vyskytujú skúsenosti s honeypotmi vo vyučovaní informačnej bezpečnosti. V roku 2002 bol v *Gerogia Tech University* zavedený honeypot s cieľom identifikovať bezpečnostné hrozby v univerzitnej sieti. Zavedený honeypot úspešne identifikoval exploity a poukázal na zraniteľnosti, ktoré boli v rámci univerzitnej siete dovtedy nepovšimnuté. O rok neskôr bol v *Azusa Pacific University* implementovaný honeypot v rámci operačného systému Windows 2000, ktorý bol nainštalovaný bez bezpečnostných aktualizácií. Systém bol takmer okamžite zasiahnutý malvérom – počítačovým červom a botnetmi, ktoré komunikovali cez IRC kanál. *Brighamská univerzita* zaviedla v rámci výučby bezpečnostné laboratórium pre študentov informačnej bezpečnosti s názvom *ITSecLab*. Laboratórium bolo navrhnuté tak, aby študenti mohli voľne experimentovať s rôznymi bezpečnostnými nástrojmi bez rizika poškodenia reálnych informačných systémov. Mohli si tak vyskúšať skenovanie siete, analyzovanie vírusov a červov, vytváranie DoS útokov (Denial of Service) a rôzne metódy prevencie. Jedna z počítačových sietí v rámci laboratória bola nastavaná ako sandbox, ktorý úspešne bránil malvéru uniknúť zo siete a ohroziť tak funkčnú akademickú sieť. [62]

Budovanie bezpečnostných laboratórií s využitím honeypotov sa neskôr rozšírilo aj na ďalších univerzitách. S budovaním bezpečnostného laboratória sa však veľmi relevantné zdajú otázky zabezpečenia počítačovej siete, keďže prevádzka honeynetu by mala byť oddelená od bežnej prevádzky v akademickej sieti. V neposlednom rade sa vynárajú právne otázky, ktoré riešia dôsledky využitia honeypotov pri reálnej prevádzke. Tejto problematike sa budeme venovať v nasledujúcich kapitolách.

2.5 Analýza využitia honeypotov vo výučbe informačnej bezpečnosti

Jedným z hlavných cieľov tejto práce je analyzovať využitie honeypotov pre výučbu informačnej bezpečnosti. Keďže vyučovacie hodiny sú často obmedzené nielen časovým

[61] López, M. H., Reséndes, C. F., 2008, s. 73- 74
[62] Jones, J. K., Romney, G. W., 2004, s. 25

intervalom ale aj počtom zariadení, s ktorými môžu študenti pracovať, rozhodli sme sa do analýzy zahrnúť honeypoty, ktoré sú vhodné na virtualizáciu, jednoduché na inštaláciu a údržbu. V tabuľke č. 5 je zobrazená analýza vybraných honeypotov pre účely výučby.

Tab. 5 Analýza využitia vybraných honeypotov v rámci výučby

Názov honey-potu	**Oblasť**	**Kategória**		**Popis základnej činnosti**	**Použitie pri výučbe informačnej bezpečnosti**
		Podľa miery inter-akcie	Podľa smeru inter-akcie		
Kippo	SSH	stredná miera inter-akcie	server	Zaznamenáva útoky na SSH server, emuluje prostredie reálneho SSH servera, zachytáva všetky príkazy ktoré vykonal útočník v emulovanom prostredí honeypotu	Útoky hrubou silou a slovníkové útoky
					Bezpečnosť zvoleného hesla
					Bezpečnosť SSH servera
Glastopf	Web	nízka miera inter-akcie	server	Emuluje zraniteľnosti webových aplikácií (SQL Injection a iné), odpovedá útočníkovi na HTTP požiadavky.	Bezpečnostné útoky na webové aplikácie
					Dôveryhod-nosť rôznych typov webových stránok

Názov honey-potu	Oblasť	Kategória		Popis základnej činnosti	Použitie pri výučbe informačnej bezpečnosti
		Podľa miery inter-akcie	Podľa smeru inter-akcie		
					Pishing
Dionaea	Sieťové služby	nízka miera inter-akcie	klient	Emuluje rôzne zraniteľnosti v závislosti od ponúkaných sieťových služieb. Cieľom je získať kópiu malvéru.	Malvér a jeho kategorizácia
					Bezpečnostný útok a útočník
Stack Honeypot	Spam	nízka miera inter-akcie	server	Vystupuje ako webová stránka lákajúca spambotov	Spam a ochrana pred spamom
Google Hack Honeypot	Vyhľa-dávač Google	nízka miera inter-akcie	server	Skúma prieskumné útoky vedené prostredníc-tvom vyhľadávača Google (tzv. google hacks)	Prieskumné útoky
					Zverejňovanie osobných údajov
Shadow daemon	Web	vysoká miera	server	Súbor nástrojov na detekciu webových útokov, slúži aj	Firewall

Názov honey-potu	Oblasť	Kategória		Popis základnej činnosti	Použitie pri výučbe informačnej bezpečnosti
		Podľa miery inter-akcie	Podľa smeru inter-akcie		
		inter-akcie		ako firewall, ktorý odchytáva podozrivé aktivity	Bezpečnosť webových aplikácií
Honeypot Camera	Hardvér	nízka miera inter-akcie	server	Skúma podozrivé aktivity prichádzajúce na webovú kameru	Typy útočníkov a spôsoby útokov.
High Interaction Honeypot Analysis Toolkit	Web	vysoká miera inter-akcie	server	Vytvorí z akýchkoľvek webových aplikácií honeypot	Bezpečnosť webových aplikácií.
Ghost USB Honeypot	Hardvér	nízka miera inter-akcie	klient	Emuluje USB kľúč.	Šírenie malvéru cez USB.
Conpot	SCADA systémy	nízka miera inter-akcie	server	Emuluje rôzne SCADA systémy.	Analýza útokov na SCADA systémy

Z hľadiska účelu ide o výskumné honeypoty. Z pohľadu interakcie sú takmer všetky honeypoty s nízkou mierou interakcie. Okrem toho, že nasadenie honeypotov s vysokou mierou interakcie prináša so sebou väčšie riziko zneužitia, poskytuje kópiu reálneho systému. Honeypoty s nízkou mierou interakcie sú vhodnejšie pre účely výučby, keďže sú určené na konkrétnu službu, resp. účel.

Niektorým z uvedených honeypotov sme venovali pozornosť aj v našej práci. Vybrali sme pre náš výskum honeypoty, ktoré sme považovali za najvhodnejšie pre výučbu informačnej bezpečnosti. Následne sme zostavili didaktické materiály zodpovedajúce konkrétnym modulom výučby informačnej bezpečnosti pomocou uvedených honeypotov.

Okrem vyššie uvedených honeypotov s honeypotmi úzko súvisia nástroje, ktoré sú spoločne s nimi vyvíjané. Ide napríklad o **honeymapu** [63], ktorá zobrazuje pôvod útokov na honeypoty. Túto mapu je možné ukázať pri ukážkach početnosti útokov a ako peknú vizualizačnú pomôcku o dôležitosti informačnej bezpečnosti. Druhým nástrojom je **Cuckoo sandbox.**[64] Tento automatizovaný nástroj vytvára uzavretý priestor pre testovanie rôznych typov malvéru. Využíva najmä vzorky získané z honeypotov Dionaea a Kippo. Alternatívou k tomuto nástroju je online verzia Cuckoo sandboxu – služba **Malwr.** [65]

[63] https://github.com/fw42/honeymap
[64] https://www.cuckoosandbox.org/
[65] malwr.com

3 Koncept laboratória informačnej bezpečnosti

V tejto kapitole navrhneme funkčné laboratórium informačnej bezpečnosti, ktoré bude slúžiť na výučbu žiakov v tejto dynamicky sa rozvíjajúcej oblasti. Vyhodnotíme vstupné požiadavky pre účastníkov kurzu informačnej bezpečnosti, zameriame sa na stanovenie cieľov výučby a presný popis laboratórneho prostredia, v ktorom budú žiaci pracovať. Povieme si aj o rôznych aspektoch využitia takéhoto laboratória na akademickej pôde. V neposlednom rade vyhodnotíme výsledky praktickej realizácie vstupného testu a vyvodíme z nich konkrétne závery, ktoré v konečnom dôsledku určite ovplyvnia postoj vyučujúceho k výučbe informačnej bezpečnosti.

3.1 Popis laboratória informačnej bezpečnosti

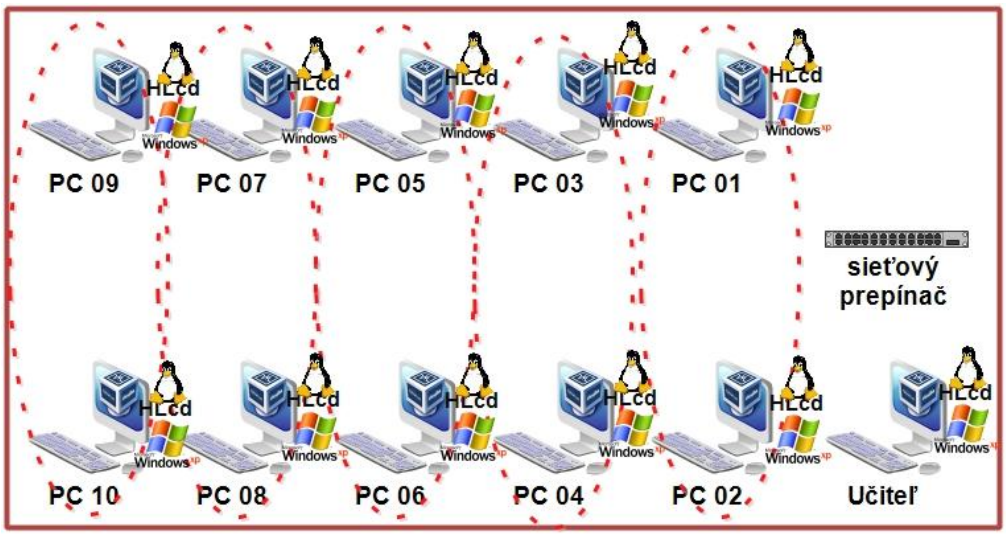
Pri výučbe informačnej bezpečnosti vychádzame z predpokladov, že na škole sa nachádza počítačové laboratórium s minimálne jedenástimi (desať počítačov pre žiakov a jeden pre vyučujúceho). Na obrázku č 3. sme schematicky znázornili laboratórium. Odporúčame, aby sa pri výučbe informačnej bezpečnosti využívali výhody, ktoré prináša koncept virtualizácie. Virtualizácia ako taká umožňuje spúšťať na tom istom počítači niekoľko informačných systémov odlišných v závislosti od typu virtualizácie. V rámci návrhu sme použili ako virtualizačný nástroj VirtualBox.[66] Bližšie si o ňom povieme v nasledujúcich častiach tejto práce. Ďalšou a nemenej známou výhodou virtualizácie je neznehodnotenie operačného systému, ktorý je nainštalovaný na počítači a vytváranie tzv. bodov obnovy v prípade znehodnotenia operačného systému. Pod znehodnotením systému myslíme jeho následnú nemožnosť využiť ho ďalej v rámci výučby. To sa môže stať v prípade testovania rôznych vzoriek škodlivého kódu. Ako virtuálne stroje odporúčame použiť operačný systém ***Windows XP*** a nami navrhnutú live distribúciu ***HoneypotLearningLiveCD*** (HLL CD). HLL CD rozoberieme v nasledujúcej časti práce. Samozrejme, je možné namiesto Windows XP využiť aj iný operačný systém. Výber takého operačného systému by mal spĺňať nasledujúce parametre:

- nízke hardvérové nároky,
- prostredie známe pre žiakov

[66] https://www.virtualbox.org/

Ďalším problémom v tomto smere môže byť otázka licencií. V tomto smere je možné uvažovať o využití licencií Microsoft MSDN[67] a Microsoft Campus Agreement[68].

Počítače sú navzájom prepojené pomocou sieťového prepínača. Nie je nutné, aby sieťový prepínač bol manažovateľný. Dôležité je, aby učiteľ v prípade problémov vedel dočasne odpojiť ten sieťový port, ktorý prináleží konkrétnemu počítaču. Ako je možné vidieť na obrázku č. 3 , počítače by mali byť usporiadané tak, aby žiaci mohli navzájom spolupracovať (napr. PC01 a PC02, PC03 a PC04). Odporúča sa, aby za jedným počítačom boli maximálne dvaja žiaci. Niektoré úlohy sú pripravované tak, aby bol žiak, resp. žiaci za jedným počítačom v role útočníka a žiak, resp. žiaci za druhým počítačom v role obete. V ďalšej úlohe si tieto role môžu vymeniť.



Obr. 3 Schéma laboratória

3.2 Honeypot Live Learning CD (HLL CD)

Ako už bolo vyššie spomenuté, súčasťou tejto práce je aj vytvorenie live CD, ktoré obsahuje všetky potrebné nástroje použité v tejto práci. Toto live CD je možné nájsť vo formáte *.iso* na priloženom DVD k tejto práci.

HLL CD pozostáva z operačného systému Debian LXDE a z nástrojov, ktoré použijeme vo výučbe informačnej bezpečnosti. Systém bol vytvorený tak, aby využíval maximálne 512 MB systémovej pamäte. Toto live CD obsahuje nasledujúce nástroje, ktoré budeme aktívne využívať pri výučbe informačnej bezpečnosti:

[67] https://www.microsoft.com/slovakia/msdn/
[68] https://www.minedu.sk/9948-sk/microsoft- campus-agreement- zmluva-microsoft- campus-and-school/

- **Ncrack** – nástroj určený na vykonávanie slovníkového útoku[69],
- **Nmap** – nástroj určený na skenovanie počítačovej siete[70],
- **Hydra** – nástroj určený na vykonanie brute force útoku[71],
- **OpenSSH server** – nástroj na vzdialený prístup k systému[72]
- **Kippo** – honeypot, ktorý zbiera informácie o útokoch na SSH server[73],
- **Kippo Graph** – nástroj na vizualizáciu dát zachytených pomocou Kippo honeypotu.[74]

3.3 Webový portál na výučbu informačnej bezpečnosti

Okrem live CD sme v práci vytvorili aj portál pre výučbu informačnej bezpečnosti. Vytvorený webový portál slúži nielen na realizáciu fixačných a diagnostických častí vyučovacej hodiny. Obsahuje aj definície pojmov a návody na prácu s rôznymi nástrojmi, či už s honeypotom, s nástrojmi, ktoré študenti budú používať na útočenie, ale aj so samotnými virtuálnymi operačnými systémami.

Podmienkou pre vstup do portálu je úspešná registrácia, v ktorej študent vyplní svoju prezývku, e-mailovú adresu a zvolené heslo.

Obr. 4 Registrácia do webového portálu informačnej bezpečnosti

[69] https://github.com/nmap/ncrack
[70] https://nmap.org/
[71] https://www.thc.org/thc-hydra/
[72] http://www.openssh.com/
[73] https://github.com/desaster/kippo
[74] https://github.com/ikoniaris/kippo-graph

Po úspešnej registrácii a prihlásení si študent môže zvoliť jeden z modulov, ktorý predstavuje konkrétnu metodiku výučby informačnej bezpečnosti.

Obr. 5 Výber modulu informačnej bezpečnosti

Každý z modulov obsahuje viaceré typy úloh a rovnako aj definície z oblasti informačnej bezpečnosti. Text označený jablkom obsahuje nové a dôležité informácie, ktoré študenti využijú pri výučbe informačnej bezpečnosti aj pri vypĺňaní kvízových otázok, či praktických úloh. Ceruzkou je označený vedomostný kvíz a hviezdou sú označené praktické úlohy.

Obr. 6 Modul Bezpečnostný útok a útočník

Jednotlivé úlohy vyzerajú nasledovne :

Obr. 7 Modul Malvér a kategorizácia malvéru

Motiváciou študentov je získať čo najväčší počet bodov a otvoriť tak nový modul informačnej bezpečnosti, v ktorom sa dozvedia ďalšie, rozširujúce poznatky o informačnej bezpečnosti.

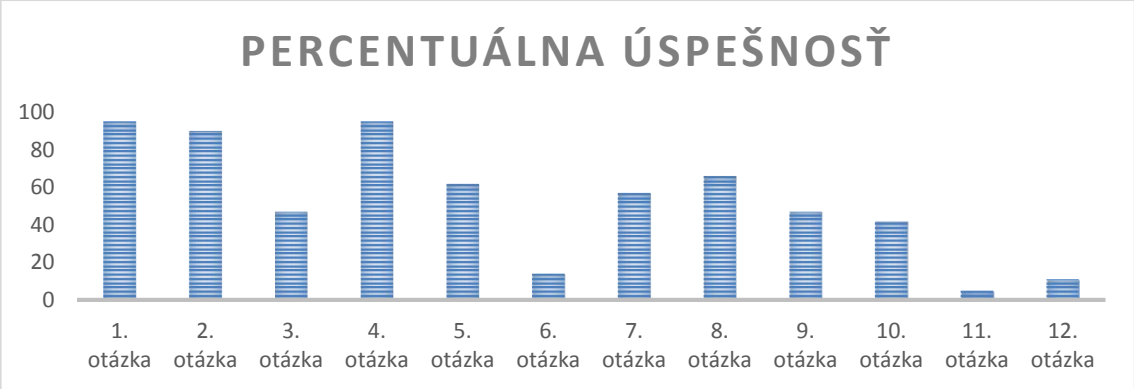
3.4 Vstupné vedomosti žiakov

Vstupné vedomosti žiakov môžu byť rôznorodé. Závisia od viacerých faktorov, či už vekového rozpätia žiakov, absolvovaného učiva či individuálneho prístupu vyučujúceho, ktorý môže rozšíriť zoznam vedomostí a zručností žiakov o ďalšie samostatne zvolené štandardy. Na to, aby študent vedel pracovať s jednotlivými honeypotmi potrebuje širokú znalosť ovládania operačného systému, prípadne sieťových služieb, ktoré sú v rámci neho konfigurované. Vytvorené laboratórium informačnej bezpečnosti zahŕňa aj prácu s virtualizačným softvérom, preto tiež očakávame, že sa študent bude dobre orientovať v jeho prostredí a nastaveniach.

Úlohou vstupného testu bolo vyhodnotiť vedomostnú úroveň žiakov, ktorí majú k informačnej bezpečnosti najbližšie – ako testovaciu vzorku sme vybrali študentov Strednej odbornej školy Ostrovského 1 v Košiciach s odborom Mechanik počítačových sietí. Vedomosti testovacej vzorky preto predstavovali maximálny okruh vedomostí z informačnej bezpečnosti. Žiaci samozrejme nemuseli zodpovedať na všetky otázky správne, cieľom bolo stanoviť

dosiahnutý level vedomostí ako maximálnu hranicu a na základe nej stanoviť nasledujúci postup vo výučbe informačnej bezpečnosti. Vyhodnotenie však ukázalo, že sme hranicu stanovili príliš vysoko. Nasledujúci graf predstavuje percentuálnu úspešnosť žiakov testovacej vzorky vo vstupnom teste. Vstupný test, ktorý sme pre tento účel vytvorili, sa nachádza v prílohe *Vstupný test*. Test pozostáva z otvorených otázok s krátkou odpoveďou a z uzatvorených otázok s výberom odpovede. Úlohy sú zamerané nielen na definovanie pojmov vlastnými slovami, ale aj na riešenie problémových situácií, ktoré by študenti v rámci výkonu svojho budúceho povolania mali ovládať.

Graf. 3 Percentuálna úspešnosť študentov – vstupný test



Z grafu môžeme vyčítať, že najviac študentov odpovedalo správne na otázky týkajúce sa pojmov útočník a zraniteľnosť informačného systému, zatiaľ čo najmenej správnych odpovedí sme zaznamenali pri posledných dvoch otázkach vstupného testu, ktoré sa venovali praktickým riešeniam problémov informačnej bezpečnosti, ako je ochrana pred konkrétnym typom malvéru alebo účinný postup na ochranu webového servera pred útočníkom, ktorý môže využiť existujúcu zraniteľnosť chybného skriptu. Posledné otázky síce boli uzavreté s výberom odpovede, ale študenti museli svoju odpoveď stručne odôvodniť, vďaka čomu sme predišli náhodným typom správnych odpovedí.

Na základe výsledkov vstupného testu môžeme konštatovať, že vyučujúci, ktorý pracuje so študentami najlepšie dokáže odhadnúť rozsah ich vedomostí a zručností. Testovacia vzorka ukázala, že hranica vedomostí sa odlišuje nielen podľa odboru študentov, ale aj podľa osobitného prístupu študenta k vybranej kapitole učiva. Do vstupného testu sme zahrnuli otázky, ktoré boli pre študentov v testovacej vzorke náročné, často mali problém porozumieť otázke a niekedy došlo aj k technickým problémom spôsobeným systémom Moodle,

prostredníctvom ktorého študenti vypĺňali vstupný test. Tieto problémy potom ubrali na motivácii študentov odpovedať na zadanú otázku čo možno najpresnejšie, prípadne svoju odpoveď odôvodniť primeraným spôsobom. Vytvorený vstupný test preto navrhujeme pozmeniť nielen v jeho zložitosti ale aj v spôsobe realizácie. Kľúčové pojmy vstupného testu, na základe ktorých sú vytvorené otázky pre študentov, by mali byť výsledkom prieniku vedomostí študentov zo stredných odborných škôl a gymnázií. Vzhľadom na pojmy a kompetencie študentov uvedené v Štátnych vzdelávacích programoch, by sme odporúčali orientovať vstupný test na pojmy ako malvér, antivírusový softvér, vírus, trójsky kôň, spam, netiketa, útočník, bezpečnostný útok, firewall alebo sa zamerať priamo na konkrétne prístupy orientované na zabezpečenie počítačovej siete, ktoré by zvládol aj študent – laik.

4 Výučba informačnej bezpečnosti

V tejto kapitole si predstavíme metodiky výučby informačnej bezpečnosti. Metodiky budú venované naplneniu hlavne kognitívnych, psychomotorických a afektívnych cieľov, ktoré sme si určili v predchádzajúcej kapitole. Sú vytvorené s ohľadom na očakávané vstupné vedomosti a zručnosti študentov, s cieľom naučiť ich pracovať s rôznymi nástrojmi pre lepšie pochopenie pojmov z informačnej bezpečnosti.

4.1 Modul č. 1: Výučba pojmov bezpečnostný útok a útočník

Študenti často vedia vlastnými slovami vysvetliť čo je to bezpečnostný útok a kto je to útočník, málokedy si však vedia predstaviť ako bezpečnostný útok prebieha a aké metódy či postupy môže útočník zvoliť na realizáciu bezpečnostného útoku. Preto sme ako prvú vytvorili metodiku výučby, v rámci ktorej si študenti môžu vyskúšať rolu útočníka a obete a taktiež niektoré bezpečnostné útoky zamerané na SSH server.

4.1.1 Stanovenie didaktických cieľov a metód použitých pri výučbe

Nasledujúca tabuľka predstavuje kognitívne, psychomotorické a afektívne ciele, ktorých naplnenie očakávame po realizácii tejto metodiky vo výučbe informačnej bezpečnosti.

Tab. 6 Didaktické ciele a metódy – metodika č. 1

Kategória	Cieľ	Použité didaktické metódy
Kognitívne ciele	Na základe praktickej ukážky vlastnými slovami definovať bezpečnostný útok.	Výklad formou prezentácie alebo inej zvolenej metódy.
	Kategorizovať bezpečnostný útok podľa stanovených kritérií.	
	Vlastnými slovami vysvetliť rozdiel medzi	

Kategória	Cieľ	Použité didaktické metódy
	brute force a slovníkovým útokom.	
	Definovať pojem útočník.	
	Analyzovať bezpečnosť zvoleného hesla v závislosti od jeho dĺžky a obsiahnutých znakov.	
Psychomotorické ciele	Vykonať brute force útok na SSH server	Demonštračná metóda formou praktickej ukážky bezpečnostného útoku.
	Vykonať slovníkový útok na SSH server	
	Na základe informácií z honeypotu charakterizovať útočníka, ktorý vykonal útok na SSH server	
Afektívne ciele	Zamyslieť sa nad bezpečnosťou používaných hesiel.	

4.1.2 Motivačná časť

Najčastejšími útokmi z reálneho života sú útoky na služby využívajúce SSH protokol. Bohužiaľ, študenti sa často nestretávajú s SSH serverom, preto je vhodné motivovať ich situáciou, ktorú poznajú z bežného života, či už ide o bezpečnosť operačného systému, ktorý používajú doma vo svojom osobnom počítači, alebo bezpečnosť školského servera, ktorý slúži na posielanie domácich úloh a evidenciu známok študentov.

4.1.3 Expozičná časť

Bezpečnostný útok chápeme ako vedomý alebo nevedomý čin, ktorý môže viesť k poškodeniu alebo ku zneužitiu informácií a informačných systémov, voči ktorým je cielený. Bezpečnostné útoky môžu byť aktívne alebo pasívne, úmyselné alebo neúmyselné, či priame alebo nepriame. Príkladom pasívneho útoku je, keď sa napríklad náhodou dozvieme citlivé

informácie, ktoré nie sú určené pre nás. Naopak, ak sa snažíme cielene preniknúť do informačného systému a získať takéto informácie, ide o úmyselný, priamy a aktívny útok. Príkladom neúmyselného útoku je úder blesku po ktorom informačný systém zasiahne požiar. Nepriamo a nevedome sa stávame súčasťou bezpečnostného útoku, ak je náš počítač súčasťou siete botnetov, ktorú ovláda útočník a využíva napríklad na uskutočňovanie DDos útokov. [75]

V rámci SSH servera študentom predvedieme dva typy bezpečnostných útokov, zameraných na získanie prístupového hesla SSH servera. Prvým z nich je **brute force útok**, ktorý sa nazýva aj útok hrubou silou. Jeho cieľom je spomedzi všetkých kombinácii znakov odhaliť správnu kombináciu, ktorá predstavuje hľadané heslo. Takéto spôsoby útočenia sú náročné nielen na čas ale aj na potrebné zdroje a navyše nie sú efektívne, nakoľko často sa v rámci bezpečnosti systému stanovuje maximálny počet prihlásení s nesprávnu kombináciou hesla**. Slovníkový útok** je variáciou brute force útoku, v ktorom sa zužuje počet vyskúšaných kombinácií vzhľadom na najčastejšie používané kombinácie používateľských mien a hesiel, ktoré sú uložené v tzv. slovníkovom súbore. Administrátor informačného systému však môže tento súbor použiť na to, aby používateľom zakázal zvoliť si jednoduché heslá a zabrániť tak neoprávnenému prístupu do informačného systému. [76]

Útočník, v slangovom výraze známy od začiatku 80. rokov ako *hacker* je označenie pre osoby zaoberajúce sa počítačovou kriminalitou. V súčasnosti poznáme viacero kategorizácií útočníkov, azda najznámejšie rozdelenie je pomerne metaforické, podľa farby klobúka, v prenesenom význame podľa úmyslu, na základe ktorého útočník vykoná svoj útok. Takto rozdeľujeme útočníkov na *White Hat* – je útočník, ktorý je zvyčajne správca informačného systému, profesionál v oblasti informačnej bezpečnosti, jeho cieľom je získať informácie o zraniteľnostiach v informačnom systéme, ktorý spravuje. Opakom je *Black Hat* – ten narúša informačnú bezpečnosť so zlým úmyslom, s cieľom poškodiť dáta alebo vyradiť informačný systém z prevádzky. Hlavný rozdiel medzi týmito dvoma kategóriami tvoria práva – zatiaľ čo prvý typ útočníka má plnú autorizáciu v systéme a jeho útočenie je v medziach zákona, druhý typ útočníka praktikovaním bezpečnostných útokov vykonáva nezákonnú činnosť. Kategória *Gray Hat* stojí na pomedzí týchto dvoch typov – predstavuje etického útočníka, ktorý síce nemá oprávnenia administrátora systému, ale po úspešnom útoku informuje správcu systému o zistených zraniteľnostiach.[77]

[75] porov. M. Whitman, H. Mattord, 2011, s. 9
[76] porov. M. Whitman, H. Mattord, 2011, s. 67
[77] porov. L. A. Long, 2012, s. 5-6

4.1.4 Fixačná časť

V rámci fixačnej časti výučby sme pre študentov vytvorili pracovný list, ktorý obsahuje základné pokyny na prácu s SSH serverom, s nástrojmi Ncrack a Hydra a s honeypotom Kippo SSH. Pracovný list sa nachádza v prílohách tejto práce a jeho praktické overenie vo výučbe spomenieme v kapitole, ktorá pojednáva o skúsenostiach z praktickej aplikácie vytvorených metodík. Pracovný list bol vytvorený pre potreby konkrétnych študentov, ktorí absolvovali výučbu na základe tejto metodiky. Je možné ho však aplikovať aj na vyučovacích hodinách, pri ktorých študenti disponujú inými vstupnými vedomosťami ako vybraná skupina študentov.

Vytvorený pracovný list pozostáva z dvoch častí. Prvá časť je zameraná na praktickú prácu s SSH serverom, nakoľko testovacia skupina nedisponovala vedomosťami o základných funkciách a spravovaní SSH servera. Obsahuje aj úlohy týkajúce sa práce s prostredím virtualizačného programu VirtualBox a taktiež úlohy na spustenie slovníkového útoku pomocou nástroja Ncrack. V druhej časti pracovného listu je priestor nielen na prácu s Honeypotom, ale aj s nástrojom Hydra určeným pre brute-force útok. Pracovný list však nie je zameraný na samostatnú prácu žiakov, ideálne je ak pracujú vo dvojiciach a v prípade otázok je v blízkosti aj vyučujúci, ktorý ich usmerní kde a akým spôsobom hľadať správne odpovede.

Prvá úloha je zameraná na prácu s virtualizačným softvérom. Študenti majú za úlohu importovať obraz virtuálneho operačného systému podľa návodu uvedeného v tretej kapitole, ktorý je taktiež priložený na webovej stránke, ktorú sme vytvorili na tento účel. Ich úlohou je aj zamyslieť sa nad tým, prečo je potrebné zmeniť MAC adresu importovaného zariadenia. Keďže pracujeme s tým istým obrazom ktorý sa importuje na viaceré zariadenia, je potrebne urobiť tento úkon, aby sa následne pridelené IP adresy navzájom odlišovali a aby nedochádzalo k chybám pri posielaní paketov.

V druhej úlohe sa študenti oboznámia s prostredím virtuálneho operačného systému. Ich úlohou je zmeniť prístupové heslo pre konto *student*, a to s použitím príkazu *passwd*. Študenti sú upozornení, aby nedošlo k omylu a nezmenili heslo v konte *root*.

Tretia úloha súvisí so zistením IP adresy, študenti si vďaka tejto úlohe uvedomia význam IP adresy v sieťovej komunikácii, keďže ju ďalej budeme potrebovať na komunikáciu s SSH serverom.

V ďalšej úlohe sa majú študenti prihlásiť priamo na SSH server svojho spolužiaka, teda si vyskúšajú potrebný príkaz a pokúsia sa analyzovať, aké parametre príkaz obsahuje. Všimnúť si môžu hlavne parameter *–p*, ktorý definuje číslo portu, na ktorom počúva SSH server. Úlohou študentov je po úspešnom prihlásení vytvoriť priečinok v domovskom adresári svojho

spolužiaka. Na to použijú príkaz *mkdir*. Zároveň si vyskúšajú odhlásenie sa z pripojeného SSH servera príkazom *exit*.

V piatej úlohe študenti zistia, kde sa nachádza konfiguračný súbor SSH servera a jeho absolútnu cestu si zaznačia do pracovného listu. Ide o súbor */etc/ssh/sshd_config,* v ktorom máme možnosť zmeniť si číslo portu, na ktorom bude počúvať SSH server. Cieľom úlohy je zmeniť prednastavené číslo portu 6666 na port 22, na ktorom štandardne počúva SSH server. Študenti majú za úlohu zakrúžkovať činnosti, ktoré vykonali počas zmeny portu – išlo hlavne o prihlásenie sa pod administrátorským účtom *root* a editáciu súboru v editore *nano*.

V ďalšej úlohe mali študenti zistiť príkazy, pomocou ktorých reštartujeme SSH server po úspešnej zmene v konfiguračnom súbore. Ide o príkaz *service ssh restart*, ktorý je možné spustiť len pod administrátorským účtom.

Ak študenti správne zmenili číslo portu z 6666 na port 22, nebude potrebné v siedmej úlohe pri prihlasovaní na SSH server zadávať parameter p, keďže port 22 je štandardným portom pre SSH server.

V ôsmej úlohe študenti použijú nástroj *nmap* na preskenovanie portov, ktoré má spolužiak povolené v rámci svojho operačného systému. Dôležité je, aby si všimli, že pri porte 22 sa nachádza aj popis služby, ktorá je pre tento port štandardná – teda SSH server. Takto nastavený port je vlastne pozvánkou pre útočníka, aby vyskúšal niektoré typy útokov zameraných na SSH server, keďže má presnú informáciu o otvorenom porte číslo 22. Použitie nástroja *nmap* môžeme radiť medzi prieskumné útoky, ktoré často otvárajú cestu ďalším, nebezpečnejším krokom útočníka.

V deviatej úlohe si študenti vyskúšajú prácu s nástrojom *Ncrack*, pomocou ktorého môžu vykonávať slovníkový útok na SSH server. Vďaka tejto úlohe dokážu študenti predvídať, kedy je slovníkový útok úspešný a na základe akého princípu funguje. Buď si ich spolužiak zvolí jedno z hesiel v slovníku, alebo zapíšu jeho existujúce heslo na niekde na začiatok slovníka. Z toho vyplýva, že slovníkový útok bude úspešný len vtedy, ak sa reálne nastavené heslo skutočne nachádza v slovníku. Študenti majú taktiež možnosť podrobne analyzovať heslá, ktoré sa nachádzajú v slovníku. Môžu si všimnúť, na základe akých kombinácií znakov sa heslo stáva jednoduchým a predvídateľným. V tejto úlohe si uvedomia dôležitosť zvolenia silného hesla nielen pri konfigurácií SSH servera ale aj pri používaní iných sieťových služieb.

Desiata úloha je zameraná na priame vykonanie slovníkového útoku. Študenti si vďaka zadanému príkazu uvedomia, čo všetko potrebuje útočník k úspešnému slovníkovému útoku – port, na ktorom počúva napadnutá sieťová služba, IP adresa cieľového zariadenia,

používateľské meno konta, na ktoré útočia (v našom prípade je to konto student, avšak kľudne môže byť útočník predvídavý a rovno útočiť na administrátorské konto root), ďalej je potrebný slovník hesiel, ktorý si útočník môže vytvoriť sám, prípadne efektívnejšie stiahnuť z Internetu.

A napokon, finálna úloha prvej časti je zameraná na vyhľadávanie na Internete, študenti majú za úlohu vyhľadať názvy podobných nástrojov, ako je nástroj Ncrack a zapísať si ich do pracovného listu. Určite sa medzi nájdenými nástrojmi vyskytne aj nástroj Hydra, ktorý budeme neskôr používať v ďalšej časti pracovného listu.

Druhá časť pracovného listu je zameraná na ochranu pred útočníkom pomocou Kipppo honeypotu. Kippo honeypot je hoenypot, ktorý dokáže emulovať funkčný SSH server, pre útočníka je však táto emulácia pascou, namiesto toho, aby spôsobil škodu nášmu systému, bude jeho činnosť podrobne zaznamenaná v logoch Kippo honeypotu a pre študentov jasne a zrozumiteľne zobrazená prostredníctvom nástroja Kippo Graph.

Prvá úloha druhej časti je zameraná na zopakovanie si krokov z predchádzajúcej časti pracovného listu. Študenti majú za úlohu zmeniť číslo portu, na ktorom počúva SSH server z portu 22 na ľubovoľné iné číslo, hlavne preto, aby honeypot Kippo vedel na porte 22 simulovať pre útočníka falošný SSH server.

V druhej úlohe sa študenti oboznámia s konfiguračným súborom honeypotu Kippo. Kippo bude počúvať na porte, ktorý je uvedený v konfiguračnom súbore kippo.cfg. Ide o port 6665, na ktorý bude neskôr v nasledujúcich úlohách presmerovaná komunikácia z portu 22.

V nasledujúcej úlohe sa študenti stretnú s pojmom firewall. Ich úlohou bude zistiť viac informácií o štandardnom linuxovom firewalle s názvom *iptables*. Študenti majú za úlohu pridať do *iptables* pravidlo, ktoré presmeruje všetky pakety prichádzajúce na port 22 do cieľového portu číslo 6665, na ktorom počúva práve Kippo honeypot. V rámci štvrtej úlohy potom majú študenti presne vyznačiť, aký krok pridaním tohto pravidla urobili.

Piata úloha smeruje k prihláseniu sa pod používateľom kippo, prostredníctvom ktorého študenti môžu spustiť Kippo honeypot. Príkaz na zmenu používateľa je štandardne príkaz su.

V priečinku, v ktorom sa nachádza aj konfiguračný súbor *kippo.cfg* študenti nájdu skript, prostredníctvom ktorého spustia činnosť honeypotu. V nasledujúcej úlohe môžu študenti poprosiť svojich spolužiakov, aby sa prihlásili na SSH server cez port 22 prostredníctvom používateľského mena root a hesla 123456, ktoré je zadané v konfiguračnom súbore Kippo honeypotu (a taktiež je možné ho zmeniť). Po úspešnom prihlásení študenti vidia pričinky a súbory klasického SSH servera, avšak jeho honeypotom emulovanej kópie. Akékoľvek

zmeny, ktoré vykonajú v rámci tohto prihlásenia neovplyvnia skutočný SSH server. Naopak, každá činnosť sa podrobne zaznamená v logoch Kippo honeypotu.

V nasledujúcej úlohe si študenti môžu pozrieť príkazy, ktoré vykonali ich spolužiaci v systéme emulovanom honeypotom. Použijú na to Kippo Graph, ktorý prijateľnou formou zobrazuje záznamy v logoch honeypotu. Študenti si tak môžu pozrieť aj grafy, ktoré zobrazujú aktivitu útočníkov v rámci honeypotu, dokonca si prehrať záznam o činnosti útočníka.

V konfiguračnom súbore *kippo.cfg* sa okrem iného nastavuje aj heslo pre používateľa root, ktorým sa útočník úspešne prihlási prostredníctvom emulovaného SSH servera. Je možné ho zmeniť, prípadne použiť viacero hesiel, ktoré sa zapíšu do súboru *pass.db*. V súbore *kippo.cfg* sa dá následne upraviť aj hostname pre emulovaný systém, taktiež je možné upraviť štruktúru priečinkov, prípadne pridať súbory, ktoré by boli pre útočníka lákavé a zvyšovali by tak hodnotu systému, na ktorý práve zaútočil.

Predposledná úloha má žiakov motivovať k hľadaniu bezpečnostných opatrení na zabezpečenie SSH servera. Je však len doplnkovou úlohou, keďže v rámci tejto metodiky sa nevenujeme priamo bezpečnosti SSH servera. Posledná úloha je zameraná na brute-force útok. Študenti nemusia na brute-force útok využiť len nástroj Hydra, ktorý sa nachádza vo virtuálnom operačnom systéme, môžu nájsť na Internete aj ďalší nástroj a následne opísať jeho činnosť svojím spolužiakom. Dôležité je, aby si študenti uvedomili, že časová náročnosť brute-force útoku je väčšia ako pri použití slovníkového útoku.

4.1.5 Diagnostická časť

Pre diagnostickú časť sme v našej práci navrhli webovú stránku, ktorá bude overovať vedomosti študentov z každého modulu. V rámci diagnostickej časti sme navrhli niekoľko úloh, ktoré overia, či študenti zachovali postup pri spúšťaní honeypotu a dosiahli ciele stanovené v úvode tejto metodiky.

Prvá otázka je zameraná na bezpečnostný útok. Študenti majú rozhodnúť, aký typ bezpečnostného útoku uskutočnili počas vyučovania na SSH server s použitím nástroja Ncrack. Na výber majú typy útokov, ktoré sme definovali v expozičnej časti. Úlohou je správne rozlíšiť či sa jednalo o aktívny alebo pasívny, úmyselný alebo neúmyselný či priamy alebo nepriamy útok. Správna odpoveď spomedzi možností je len jedna, počas vyučovacej hodiny sme vykonávali aktívne útoky, keďže sme sa aktívne snažili preniknúť do zabezpečeného systému, zároveň šlo o úmyselné útoky, keďže nám k tomu nedopomohla prírodná katastrofa alebo iné

fyzické poškodenie zariadenia, a zároveň išlo o priamy útok, keďže sme sa nestali súčasťou riadeného botnetu.

Druhá otázka diagnostickej časti je zameraná na správne zaradenie do role útočníka. Keďže sme počas vyučovacej hodiny útočili na systémy, na ktoré sme mali prístup (či už s pomocou spolužiaka alebo v rámci pôvodných nastavení systému), môžeme sa označiť za útočníkov typu White Hat.

Tretia otázka sa venuje bezpečnosti zvoleného hesla. Študenti majú na výber zvoliť si heslo na svoje školské e-mailové konto spomedzi viacerých možností. Možnosti obsahujú heslá rôznej dĺžky a s rôznymi znakmi. Študenti musia rozhodnúť, ktoré z nich by bolo najvhodnejšie, pričom existuje viacero správnych odpovedí. Svoju voľbu môžu odôvodniť v komentári k úlohe.

Štvrtá otázka znova stavia študentov do role útočníka. Študenti majú za úlohu odhadnúť, ktorý postup by bol rýchlejší pri odhaľovaní sedemmiestneho hesla. Zároveň je známe, že heslo sa nachádza v slovníku, ktorý môžeme použiť v slovníkovom útoku. Študenti majú na výber niekoľko možností. Môžu si zvoliť len nástroj Hydra na vykonanie brute force útoku. Takisto môžu individuálne použiť nástroj Ncrack na vykonanie slovníkového útoku. Existuje aj možnosť použiť obidva nástroje súčasne, avšak najefektívnejšia možnosť, a teda správne riešenie tejto úlohy je vytvorenie skriptu, ktorý upraví slovníkový súbor tak, aby obsahoval iba heslá dĺžky sedem znakov. V tom prípade sa rýchlosť slovníkového útoku výrazne zvýši.

4.1.6 Odporúčania pre pedagogickú prax

Metodika výučby pojmov bezpečnostný útok a útočník bola čiastočne realizovaná v rámci výučby predmetu Sieťové technológie na vzorke stredoškolských študentov s odborom Mechanik počítačových sietí. Výučba trvala približne 9 vyučovacích hodín, na túto metodiku sme si vyčlenili štyri vyučovacie hodiny. Výučby sa zúčastnilo 23 študentov, ktorí boli rozdelení do dvoch skupín, v prvej skupine bolo jedenásť a v druhej dvanásť študentov.

Študenti pred výučbou absolvovali vstupný test, ktorého výsledky sme uviedli v tretej kapitole. Počas realizácie metodiky sme sa dozvedeli, že študenti neovládajú pojmy ako SSH protokol či prácu s prostredím operačného systému Linux. Preto sme prispôsobili pracovný list týmto študentom na mieru, tak, aby pracovný list obsahoval aj úlohy zamerané na správu a narábanie s SSH protokolom. Hoci bolo učivo pre nich náročné, študenti prejavovali záujem dozvedieť sa nové informácie a poznatky, ktoré sa týkali preberanej témy. V rámci prvej skupiny pracoval každý žiak samostatne, naopak, v druhej skupine sme zvolili prácu vo dvojici.

Študenti pracujúci vo dvojici pracovali rýchlejšie a efektívnejšie, ako študenti, ktorí pracovali samostatne.

Odporúčame preto pedagógom, aby pri práci s pracovným listom študentov nechali pracovať vo dvojiciach prípadne v niekoľkočlenných tímoch, pričom je dôležité, aby si študenti vyskúšali nielen rolu útočníka, ale aj správcu systému na ktorého sa útočí. Študenti by mali jednotlivé úlohy pracovného list vypĺňať postupe, určite odporúčame udržať poradie prvej a za ňou nasledujúcej druhej časti pracovného listu. Niektoré úlohy pracovného listu sú doplnkové, určené pre rýchlejších študentov, ktorí práve nepomáhajú svojím slabším spolužiakom. Takéto úlohy môže učiteľ po osobnom zvážení v pracovnom liste vynechať.

Expozičná časť tejto metodiky nemusí byť podaná len formou prezentácie alebo slovného výkladu, učiteľ môže využiť viacero prostriedkov na to, aby zaradil expozičnú časť učiva do aktuálnej práce študentov, ktorí vykonávajú bezpečnostné útoky alebo riadia a konfigurujú honeypot.

4.2 Modul č. 2: Malvér a kategorizácia malvéru

Malvér je pre študentov určite známym pojmom, hoci sa im niekedy môže chybne zamieňať s pojmom vírus. Často sa aj oni sami stanú obeťou malvéru, hlavne pri surfovaní na Internete. Cieľom tejto metodiky je naučiť študentov rozlíšiť čo malvér je, ako sa správa a aké dôsledky môže mať jeho činnosť pri napadnutí operačného systému. V tejto metodike budeme používať nástroje zvané ***sandboxy***, určené na analýzu nebezpečných súborov. Zároveň využijeme virtuálny operačný systém Windows ako testovacie prostredie, aby sme študentom názorne predviedli správanie sa malvéru v bežnom, používateľskom prostredí.

4.2.1 Stanovenie didaktických cieľov a metód použitých pri výučbe

V nasledujúcej tabuľke prinášame rozdelenie kognitívnych, psychomotorických a afektívnych cieľov tejto metodiky, spolu s prislúchajúcimi didaktickými metódami, ktoré môže vyučujúci využiť pri realizácii tejto metodiky.

Tab. 7 Didaktické ciele a metódy – metodika č. 2

Kategória	Cieľ	Použité didaktické metódy
Kognitívne ciele	Definovať pojem malvér.	

Kategória	Cieľ	Použité didaktické metódy
	Vymenovať základné typy malvéru.	Výklad formou prezentácie alebo inej zvolenej metódy.
	Vlastnými slovami vysvetliť rozdiel medzi vírusom a trójskym koňom.	
	Kategorizovať malvér do navrhnutých kritérií podľa správania sa v operačnom systéme.	
	Posúdiť bezpečnosť súboru stiahnutého z Internetu.	
	Posúdiť bezpečnosť vybraných webových stránok.	
Psychomotorické ciele	Analyzovať súbor prostredníctvom Sandboxu.	Demonštračná metóda formou praktickej ukážky správania sa malvéru.
	Sledovať správanie malvéru v operačnom systéme.	
Afektívne ciele	Zamyslieť sa nad bezpečnosťou súborov, ktoré sťahujeme z Internetu.	
	Oceniť úlohu antivírusového softvéru v operačnom systéme.	

4.2.2 Motivačná časť

Študentov určite zaujme problematika a skúmanie malvéru, nakoľko sa často stávajú obeťami práve takéhoto typu bezpečnostných útokov. Z praxe vieme konštatovať, že študenti si často neuvedomujú hodnotu antivírusového softvéru, používajú jeho zastarané a neaktualizované verzie, a potom sa aj dostávajú do situácií, v ktorých nevedia ochrániť svoje dáta alebo operačný systém. Nové typy malvéru neustále vznikajú, preto je dobré študentov oboznámiť aspoň so základnými typmi, o ktorých už určite počuli. Študenti mylne zamieňajú pojmy malvér a vírus, preto môžeme túto skutočnosť použiť ako motivačný príklad, ktorý nám pomôže tieto pojmy odlíšiť. Študenti zároveň často surfujú po Internete, prípadne sťahujú súbory z Internetu, pričom ani netušia, či ide o bezpečný súbor. Vďaka Sandboxu, ktorý si ukážeme v tejto metodike je možné zvolený súbor či webovú stránku analyzovať a pozrieť sa

zároveň na viaceré výsledky z hodnotenia antivírusových programov. Študentov tak môžeme motivovať k prezieravosti a opatrnosti voči súborom neznámeho pôvodu.

4.2.3 Expozičná časť

Škodlivý softvér, označovaný aj pojmom ***malvér***, hrá dôležitú úlohu pri vzniku bezpečnostných incidentov, ktoré narúšajú bezpečnosť informačného systému. Každý softvér, ktorý spôsobuje škodu pre používateľa informačného systému, pre počítač či počítačovú sieť, môžeme označiť ako malvér. Patria sem vírusy, trójske kone, červy, ransomware či spayware. Malvér je niekedy náročné kategorizovať, nakoľko neustále vznikajú nové typy malvéru, ktoré využívajú rôzne bezpečnostné hrozby a zraniteľnosti informačných systémov. Zraniteľnosti rôznych softvérov, ktoré ešte neboli zdokumentované bezpečnostnými odborníkmi, nazývame aj ***zero-day zraniteľnosti***. Práve tie sú často pre novovznikajúci malvér otvorenou možnosťou, ako sa čo najefektívnejšie preniknúť do informačného systému. [78]

Zo spomenutých typov malvéru sme si vybrali tie najčastejšie, s ktorými sa môžu študenti často stretnúť. Ako prvý typ si spomenieme malvér zvaný vírus. ***Vírus*** je škodlivý softvér, ktorý kopíruje sám seba bez vedomia používateľa. Na svoje šírenie však potrebuje iný, hostiteľský softvér, ktorý si používateľ operačného systému stiahne z Internetu a spustí u seba v počítači. Môžeme teda konštatovať, že vírus potrebuje „našu pomoc“ aby sa úspešne nainštaloval a infikoval náš počítač. ***Červ*** je taktiež typ malvéru, ktorý sa samostatne kopíruje bez toho, aby používateľ systému túto činnosť zaznamenal. Na rozdiel od vírusu však červ nepotrebuje našu asistenciu a skopíruje sa sám prostredníctvom počítačovej siete. Stačí, ak je aspoň jeden z počítačov nakazený týmto červom a aktívne komunikuje v rámci počítačovej siete aj s ostatnými počítačmi. ***Trójsky kôň*** patrí taktiež k najrozšírenejším typom malvéru. Jeho označenie súvisí s gréckou mytológiou, v ktorej je známy ako vojnová lesť grécky vojakov, vďaka ktorej porazili svojich nepriateľov. Tak aj malvér, ktorý je takto pomenovaný, slúži ako lesť pre používateľa operačného systému. Vystupuje totiž ako užitočný softvér, môže predstierať, že skenuje prítomnosť iného malvéru alebo vykonáva iné užitočné zmeny v operačnom systéme. V skutočnosti však tento softvér môže pôsobiť ako ***backdoor,*** teda ako zadné vrátka pre útočníka, ktorý tak so systémom môže kedykoľvek komunikovať a preniknúť doň, alebo môže zbierať dáta o používateľovi a zasielať ich útočníkovi. V niektorých prípadoch

[78] K. Kendall, Ch. McMillan, 2007, s. 29

sa z trójskeho koňa môže stať ***logická bomba***, vtedy softvér vykoná škodlivú činnosť presne vo chvíli, ktorú mu určí útočník a tvorca malvéru. [79]

Ďalším zaujímavým typom malvéru je ***ransomware***. Jeho úlohou je zašifrovať používateľovi operačného systému prístup k vlastným dátam a súborom, a to s cieľom takto vydierať používateľa. Majiteľ infikovaného počítača tak dostane svoje súbory naspäť až po zaplatení finančnej odmeny útočníkovi.[80]

Ostáva nám spomenúť význam ***analýzy malvéru.*** V súčasnosti existuje viacero prístupov, vďaka ktorým vieme kategorizovať malvér a odhadnúť, akú činnosť bude vykonávať po úspešnej inštalácii malvéru do operačného systému. Analýza malvéru nám umožňuje aj aktívne reagovať na už prebiehajúci bezpečnostný incident, identifikovať zasiahnuté a útočníkom poškodené súbory a adresáre a výsledne určiť mieru poškodenia operačného systému. Existujú dva základné prístupy k analýze malvéru – statická a dynamická analýza. Statická analýza preveruje malvér bez toho, aby bol spustený. Základná ***statická analýza*** pozostáva zo skúmania spustiteľného súboru bez toho, aby sme podrobne analyzovali inštrukcie programu. Je rýchla, ale neúčinná pre sofistikovaný malvér. Pokročilá statická analýza už analyzuje spustiteľný súbor programu podrobnou analýzou programového kódu, je časovo náročnejšia a vyžaduje dobrú znalosť programovacích jazykov. ***Dynamická analýza*** skúma malvér jeho priamym spustením a následným pozorovaním správania sa malvéru v operačnom systéme. Pri spúšťaní malvéru však musíme dbať o bezpečnosť, preto je potrebné dôkladne pripraviť prostredie, v ktorom budeme malvér spúšťať, tak aby sme predišli zbytočným rizikám či ohrozeniam systému a počítačovej siete. Pokročilá dynamická analýza používa program na spúšťanie konkrétnych inštrukcií škodlivého programu (debugger), je zameraná na detailnejšiu analýzu každého kroku, ktorý malvér vykoná v napadnutom operačnom systéme. [81]

Nesmieme zabúdať ani na ***antivírusový softvér***, ktorý by mal byť neoddeliteľnou súčasťou každého operačného systému. Ide o počítačový program, ktorý bol navrhnutý tak, aby identifikoval a odstránil malvér z nášho informačného systému. Dôležitá je pri tom jeho pravidelná aktualizácia, nakoľko pracuje s vírusovou databázou, ktorá musí byť s ohľadom na nebezpečenstvo malvéru najaktuálnejšia. Inak by sa mohlo stať, že aj vďaka zero-day zraniteľnostiam prilákame nové typy malvéru, voči ktorým sa nevieme chrániť.

[79] S. Cass, 2001, s. 60
[80] O´Gorman G., McDonald G., 2012, s. 1
[81] Kendall, Ch. McMillan, 2007, s. 29

4.2.4 Fixačná a diagnostická časť

V rámci fixačnej časti sme pre študentov pripravili niekoľko typov úloh, ktoré ich budú sprevádzať pri dynamickej analýze niektorých typov malvéru. Úlohy, ktoré sme vytvorili sú dostupné na webovej stránke nášho projektu a okrem zadania a vyhodnocovania obsahujú aj časť teórie, ktorá zodpovedá práve vybraným typom úloh.

V prvej a v druhej úlohe sa študenti stretávajú hneď s dvoma typmi malvéru – s vírusom a červom. Úlohou študentov je správne určiť či sa zadaný súbor správa ako vírus alebo zodpovedá kategórii červa. Súbory však študenti nespúšťajú priamo vo virtuálnom zariadení alebo nebodaj vo vlastnom počítači. Na to slúži nástroj sandboxu, ktorý funguje ako testovací operačný systém. Podobne ako virtuálny operačný systém, aj sandbox je odolný voči nakazeniu. Sandbox vykoná na testovacom súbore niekoľko typov analýz, urobí si dôležité záznamy o testovacom súbore, porovná existujúce databázy antivírusových programov, až napokon vynesie ortieľ o bezpečnosti alebo nebezpečenstve testovaného súboru. Študenti použijú Cuckoo Sandbox na analýzu súborov v prvých dvoch úlohách. Na základe výsledkov z prostredia sandboxu môžeme konštatovať, že súbor v prvej úlohe je vírus, ktorý sa spúšťa automaticky po naštartovaní operačného systému a ktorý vo výsledku zabraňuje používateľovi meniť registre a pridávať úlohy. Súbor druhej úlohy môžeme označiť ako červ, ktorý počúva na porte 1034.

V tretej a štvrtej úlohe už budeme vykonávať dynamickú analýzu malvéru analyzovaním súborov v prostredí virtuálneho operačného systému Windows. Študenti si v úvode uložia aktuálny virtuálny obraz systému, ktorý je zatiaľ nezasiahnutý malvérom. Pomôže nám to neskôr prinavrátiť virtuálny stroj do pôvodného stavu. Súbor, ktorý je súčasťou tretej úlohy predstavuje vírus, ktorý však nie je pre počítač veľmi nebezpečný. Po je ho spustení (presunutím súboru na otvorený príkazový riadok) vidíme sekvenciu okienok, ktoré sú zdanlivo neustále generované spolu s povzbudzujúcimi tvrdeniami o napadnutí systému. Posledné okienko však ubezpečuje používateľa operačného systému, že išlo o žart a že sa nemusí obávať. V tretej úlohe študenti opíšu text posledného okna, v ktorom sa útočník prihovoril používateľovi : *Your computer is ok...* V rámci štvrtej úlohy majú študenti znova k dispozícii vírus, ktorý vykonáva automatizovanú činnosť. V tomto prípade automaticky otvára novú kartu webového prehliadača Mozilla a smeruje ju na konkrétne video umiestnené na Youtube na URL adrese[82], ktorú študenti zadajú do riešenia štvrtej úlohy, musia ju však skopírovať z prehliadača skôr, ako bude systémová pamäť zahltená požiadavkami internetového prehliadača.

[82] https://www.youtube.com/watch?v=HSRdCBMCVzY

Nasledujúca úloha prináša študentom ukážku *trójskeho koňa*. Súbor, ktorý pretiahnutím do príkazového riadka spustíme v našom operačnom systéme, zdanlivo nič nevykoná. Ak sa však lepšie pozrieme na procesy operačného systému, zistíme, že pribudol úplne nový proces s názvom „Phantom“, ktorý bude bez toho, aby si ho bežný používateľ všimol, komunikovať s útočníkom. Ak študenti zadajú správne názov procesu, vyriešia piatu úlohu.

V poslednej, šiestej úlohe sa budeme zaoberať jedným z najnebezpečnejších typov malvéru, preto je dôležité, aby študenti so súborom pracovali opatrne. K dispozícii sú dva súbory, ktoré predstavujú možných kandidátov na *ransomware*. Po spustení súborov v testovacom prostredí sa o chvíľu zašifrujú všetky dáta uložené v priečnikoch operačného systému. Následne útočník používateľa upozorní, že sa stal obeťou ransomware. Neostáva nám nič iné, iba vrátiť virtuálny stroj do pôvodného stavu. Študenti majú v poslednej úlohe zadať počet hodín od spustenia ransomware, ktoré ostávajú používateľovi systému na vyplatenie výpalného útočníkovi. Ide o číslo 96.

4.2.5 Odporúčania pre pedagogickú prax

Rovnako, ako predchádzajúcu metodiku, aj túto sme čiastočne vyskúšali so spomenutou skupinou študentov strednej školy s odborom Mechanik počítačových sietí. Metodike boli venované dve vyučovacie hodiny, v rámci ktorých sa študenti zoznámili s prostredím sandboxu a prostredníctvom neho analyzovali správanie vybraných typov malvéru. Študenti pracovali samostatne, rýchlejší študenti pomáhali slabším pri analýze. Práca s malvérom ich zaujala a ocenili by rozšírenie výučby práve o takúto tematiku.

Túto metodiku sme predviedli aj v rámci stretnutia Klubu učiteľov informatiky, kde učitelia informatiky priamo pracovali s naším webovým portálom. Počas realizácie sme sa však stretli s niekoľkými problémami. Spôsobila ich úspešná prevencia antivírusového programu Eset NOD, ktorý zabránil jednotlivým učiteľom sťahovať škodlivý softvér z Internetu, prípadne ho sťahovať aj priamo vo VirtualBoxe. Rozhodli sme sa preto malvér uložiť priamo do virtuálneho obrazu operačného systému Windows XP.

Zároveň sa vynára otázka zabezpečenia malvéru, tak, aby študenti nemohli so škodlivými pracovať mimo virtuálneho operačného systému a nemohli ich tak zneužiť na nezákonnú a škodlivú činnosť voči inej osobe. Pre študentov je často náročná práca s virtualizačným softvérom. Ak by sa už dozvedeli, akým spôsobom zdieľať súbory medzi virtuálnym zariadením a počítačom, neznamená to, že by vedeli, ako ďalej narábať s týmto softvérom. Na druhej strane je takéhoto softvéru na Internete veľké množstvo a nie je náročné sa k nemu

dostať. Je úlohou vyučujúceho vysvetliť študentom, do akej miery je súbor predmetom skúmania a výučby, a kedy sa stáva nebezpečným nielen pre študenta ale aj pre jeho okolie.

Pedagógom odporúčame pracovať s touto metodikou pozorne. Je potrebné dbať na bezpečnosť hostiteľského operačného systému, a teda zabezpečiť prevádzku školskej, resp. akademickej siete hlavne kvalitným a aktualizovaným antivírusovým softvérom.

Záver

V predloženej práci sme si položili za hlavný cieľ analyzovať využitie honeypotov a honeynetov vo výučbe informačnej bezpečnosti pre vybranú cieľovú skupinu. V rámci praktickej analýzy sme si zvolili študentov strednej školy, ktorí mali s informačnou bezpečnosťou skúsenosti. Použitie honeypotu Kippo vo výučbe vzbudilo u týchto študentov zvýšený záujem o preberanú látku, a to aj napriek tomu, že sa s využitím SSH protokolu dosiaľ nestretli. Súčasne neboli zoznámení s prostredím operačného systému Linux a teda preberané učivo hodnotili ako náročné. Študenti pracovali samostatne aj vo dvojiciach, vyskúšali si rolu útočníka aj rolu obete útoku. Niektorí študenti pracovali samostatne, iní potrebovali pri práci s honeypotom často pomoc vyučujúceho. Záver vyučovacej hodiny bol vždy venovaný témam, ktoré študentov počas hodiny zaujali a chceli sa následne dozvedieť viac o danej problematike. Z tohto hľadiska môžeme honeypot označiť ako vhodnú didaktickú pomôcku pri výučbe informačnej bezpečnosti.

Naším cieľom bolo taktiež vytvoriť vhodné didaktické pomôcky, ktoré by moli učitelia využiť pri výučbe informačnej bezpečnosti. Spomínaný honeypot, ktorý slúžil ako názorná ukážka správania sa útočníka v operačnom systéme, sme zaradili do sady nástrojov, ktorá bola súčasťou live obrazu operačného systému, ktorý sme nazvali HLL CD (Honeypot Live Learning). Toto live CD sme využívali pri výučbe pojmov bezpečnostný útok a útočník, ktorá prebiehala efektívne vďaka možnostiam virtualizácie. Ďalej sme pre potreby druhej metodiky vytvorili virtuálny obraz operačného systému Windows XP, ktorý obsahuje vybrané vzorky malvéru. Študenti si ich tak môžu spustiť v pohodlí virtualizačného softvéru, bez toho, aby riskovali poškodenie hosťovského operačného systému. Na účely fixačnej a diagnostickej časti výučby sme pri oboch metodikách využili nami vytvorený webový portál, ktorý sprevádzal študentov jednotlivými krokmi, prinášal informácie, ktoré študenti potrebovali na správne vyriešenie zadaných úloh.

V našej práci sme vytvorili dve hlavné metodiky, ktoré sa venujú základným pojmom informačnej bezpečnosti. Prvá z nich využíva honeypot ako didaktickú pomôcku na výučbu pojmov bezpečnostný útok a útočník. Nosnou časťou tejto metodiky je okrem expozičnej časti a samotného výkladu vyučujúceho aj pracovný list, ktorý sprevádza študentov viacerými fázami – od jednoduchej práce s VirtualBoxom a SSH serverom, až po návod k použitiu nástrojov určených na útočenie a napokon, až k samotnému použitiu honeypotu ako nástroja na prilákanie a sledovanie útočníka. Druhá metodika je venovaná výučbe malvéru a jeho kategorizácii. Študenti sa často stretávajú s malvérom. Zaujíma ich, ako malvér pracuje a ako

sa správa v operačnom systéme. Na druhej strane, majú však problém rozlíšiť jednotlivé typy malvéru. V tejto metodike sme využili virtuálny operačný systém Windows XP, aby sme priamo poukázali na správanie sa malvéru v operačnom systéme. Študentom tak bolo jasnejšie, aké riziká so sebou prináša sťahovanie softvéru a rôznych súborov z neoverených zdrojov. V metodike sme zároveň použili analýzu súborov prostredníctvom nástroja Malwr, ktorý je online alternatívou ku Cuckoo Sandboxu.

Metodiky sú v rámci tejto práce začlenené do modulov. Každý modul obsahuje zároveň aj pedagogické odporúčania pre pedagógov a učiteľov, ktorí sa rozhodnú vytvorené metodiky vyskúšať v praxi. Odporúčania vychádzajú zo skúsenosti s testovacou vzorkou študentov strednej odbornej školy, ale aj zo stretnutia Klubu učiteľov informatiky. Prvú metodiku je vhodné realizovať skupinovo. Študenti tak pracujú rýchlejšie a pomáhajú si navzájom. Niektoré úlohy pracovného listu tejto metodiky sú zamerané na šikovnejších študentov, preto je možné niektoré úlohy pre krátkosť vyučovacej hodiny vynechať. Druhá metodika je vhodná na individuálnu prácu. Dôležité je upozorniť študentov na to, že pracujú s malvérom, teda s potencionálne nebezpečným softvérom. Jeho zneužitie mimo výskumné a vzdelávacie účely by za určitých okolností napĺňať znaky skutkovej podstaty trestného činu. Zároveň upozorňujeme učiteľov na dôslednosť zabezpečenia školskej, resp. akademickej sieste bezpečným a aktualizovaným antivírusovým softvérom.

V rámci tejto práce sme mali možnosť rozšíriť vedomosti študentov z informačnej bezpečnosti. Informačná bezpečnosť je v súčasnosti len okrajová zložka výučby informatiky na stredných školách, no vzrastajúci vývoj technológií a k nim prislúchajúcich bezpečnostných hrozieb, prikladá informačnej bezpečnosti na váhe. Informačná bezpečnosť v rámci vyučovania informatiky nemusí byť jednotvárna. Môžeme ju ozvláštniť praktickými ukážkami a zážitkovosťou, ktorá bude u študentov rezonovať dlhšie ako memorovaný pojem.

Zoznam použitej literatúry

1. ADEEL, M., et al., 2005. Honeynets: An Architectural Overview. In: Engineering Sciences and Technology, SCONEST 2005. Student Conference on. IEEE. p. 1-6.
2. AKSOY, P.; DENARDIS, L., 2007. Information technology in theory. Cengage Learning.
3. CASS, S., 2001. Anatomy of malice [computer viruses]. IEEE Spectrum, 38.11: 56-60.
4. ELKY, S., 2006. An introduction to information security management. Sans institute.
5. GORZELAK, K., et al., 2012. Proactive Detection of Network Security Incidents. ENISA report (A. Belasovs, Ed.).
6. GYMNÁZIUM POŠTOVÁ 9, 2015. Školský vzdelávací program [online]. Košice: Gymnázium Poštová 9. Dostupné na: https://www.gympos.sk/files/i_SkVP_GYM_POSTOVA_15-16.pdf.
7. JANOŠCOVÁ, R., 2014. Princípy informačnej bezpečnosti. Študijné materiály pre študentov. VŠM v Trenčíne, City university of Seattle.
8. JONES, J. K., ROMNEY, G. W., 2004. Honeynets: an educational resource for IT security. In: Proceedings of the 5th conference on Information technology education. ACM, p. 24-28.
9. JOSHI, R. C., ANJALI S, 2011. Honeypots: a new paradigm to information security. CRC Press.
10. KAMBOW, N., PASSI, L. K., 2014. Honeypots: The Need of Network Security. International Journal of Computer Science and Information Technologies, 5.5.
11. KENDALL, K., MCMILLAN, Ch., 2007. Practical malware analysis. In: Black Hat Conference, USA. p. 802.
12. LONG, L.A., 2012. Profiling Hackers. SANS Institute. InfoSec Reading Room, p. 1-22.
13. LÓPEZ, M. H., RESÉNDEZ, C. F., 2008. Honeypots: basic concepts, classification and educational use as resources in information security education and courses. In: Proceedings of the Informing Science and IT Education Conference.
14. MOKUBE, I., ADAMS, M., 2007. Honeypots: concepts, approaches, and challenges. In: Proceedings of the 45th annual southeast regional conference. ACM, p. 321-326.
15. O'GORMAN, G.; MCDONALD, G., 2012. Ransomware: a growing menace. Symantec Corporation.

16. OLEJÁR, D. et all. 2013. Informačná bezpečnosť. [dokument PDF] Bratislava: MF SR, december 2013. Študijné materiály pre kurzy informačnej bezpečnosti. Dostupné na: www.informatizacia.sk/vzdelavanie-voblasti-ib.
17. PELTIER, T. R., 2013. Information security fundamentals. CRC Press.
18. PROVOS, N., Holz T., 2007. Virtual honeypots: from botnet tracking to intrusion detection. Pearson Education.
19. SPITZNER, L., 2003. Honeypots: tracking hackers. Vol. 1. Reading: Addison-Wesley.
20. SPITZNER, L., 2003. The honeynet project: Trapping the hackers. IEEE Security & Privacy 1.2, s. 15-23.
21. ŠTÁTNY PEDAGOGICKÝ ÚSTAV, 2015. Inovovaný štátny vzdelávací program: Informatika – gymnázium so štvorročným a päťročným vzdelávacím programom [online]. Bratislava : Štátny pedagogický ústav, 2015. [cit. 2016.06.08] Dostupné na: http://www.statpedu.sk/sites/default/files/dokumenty/inovovany-statny-vzdelavaci-program/informatika_g_4_5_r.pdf .
22. ŠTÁTNY INŠTITÚT ODBORNÉHO VZDELÁVANIA, 2015. Dodatok č. 2, ktorým sa mení Štátny vzdelávací program pre odborné vzdelávanie a prípravu, skupinu študijných a učebných odborov 26 Elektrotechnika [online]. Bratislava: Štátny inštitút odborného vzdelávania, 2015. [cit. 2016.06.09] Dostupné na: http://www.siov.sk/files/SVP/dodatok_2_k_svp_26_elektrotechnika.pdf.
23. TAYLOR, A. 2013. Information Security Management Principles (2nd Edition). BCS The Chartered Institute for IT. Dostupné na: http://app.knovel.com/hotlink/toc/id:kpISMPE001/information-security/information-security
24. TUREK, I., 2008. Didaktika. Bratislava: Iura Edition, p. 413-415.
25. WHITMAN, M. MATTORD, H. 2011. Principles of information security. Cengage Learning, 2011. ISBN 1-111-13821-4.

Prílohy

Príloha A: Dotazník k výučbe informačnej bezpečnosti.

Príloha B: Vstupný test informačnej bezpečnosti.

Príloha C: Pracovný list - Modul č. 1

Príloha D: DVD nosič

Príloha A

Dotazník k výučbe informačnej bezpečnosti

V prvom rade by sme sa Vám chceli poďakovať za účasť na Klube učiteľov s témou Aspekty bezpečnosti vo vyučovaní informatiky. Váš názor je pre nás veľmi cenný, preto by sme Vás zároveň chceli poprosiť o spätnú väzbu, ktorá nám ďalej pomôže v našej práci.

Zvoľte typ školy:

a) Základná škola
b) Osemročné gymnázium
c) Gymnázium
d) Stredná odborná škola

Uveďte ročníky, v ktorých vyučujete informatiku (v prípade SŠ aj odbor):

_____

Koľko hodín informatiky ročne venujete informačnej bezpečnosti ?

_____

Ktoré z uvedených pojmov sú súčasťou výučby informatiky na Vašej škole?

a) malware
b) bezpečnostný útok
c) netiketa
d) bezpečnostná hrozba
e) bezpečnostné riziko
f) škodlivý softvér
g) vírus,trójsky kôň
h) hacker
i) antivírusový program
j) honeypot
k) ssh server
l) firewall
m) webový server
n) spam
o) DDoS
p) DoS
q) phishing
r) osobné údaje
s) útočník

Zvoľte možnosti, ktoré podľa Vás Vaši žiaci ovládajú:

a) Vedia rozpoznať počítač infikovaný škodlivým softvérom.
b) Vedia rozlíšiť škodlivý softvér od užitočného softvéru.
c) Vedia uviesť niektoré typy škodlivého softvéru.
d) Vedia navzájom rozlíšiť niektoré typy škodlivého softvéru.
e) Vedia posúdiť riziká nainštalovaného softvéru.
f) Vedia zabezpečiť počítač proti neoprávnenému použitiu.
g) Ovládajú prácu s antivírusovým programom.
h) Vedia zhodnotiť dôveryhodnosť informácií na Internete.
i) Vedia rozpoznať spam či podvodný email.
j) Vedia o problematike zverejňovania vlastných údajov na Internete.
k) Veda, čo sú osobné údaje a ako s nimi zaobchádzať.

Je podľa Vás potrebné rozšíriť počet hodín informatiky vzhľadom na výučbu informačnej bezpečnosti?

Áno / Nie

Aký softvér alebo iné učebné pomôcky by Ste privítali pri vyučovaní informačnej bezpečnosti?

_____

_____

Čo by Ste vylepšili na prezentovanej webovej stránke o informačnej bezpečnosti (pracovná verzia dostupná na http://s.ics.upjs.sk/~aliptajova/dp) ? Aké moduly, funkcionality, resp. príklady by Ste privítali?

_____

_____

Príloha B

Vstupný test informačnej bezpečnosti

Na nasledujúce otázky odpovedajte krátkou odpoveďou:

1. Kto je to útočník?

2. Čo je to malware?

3. Čo je to zraniteľnosť?

4. Čo je to botnet?

5. Čo je to útok?

Zvoľte z možností správnu odpoveď. Odpoveď nezabudnite zdôvodniť.

6. Počas DoS útoku správca počítačovej siete blokuje IP adresu útočníka pomocou firewallu. Útok však aj napriek tomuto opatreniu prebieha ďalej. Čo je najpravdepodobnejšou príčinou tohto problému? Vyberte jednu odpoveď.

a) malware už infikoval lokálny firewall b) útok prichádza od niekoľkých, distribuovaných hostiteľov

c) firewall nemôže blokovať DoS útoky d) potrebujeme nainštalovať antivírusový systém

7. Na hodinách informatiky učiteľ práve preberá so žiakmi správu operačného systému Linux. Preto požiadal správcu školského servera, aby vytvoril každému študentovi informatiky vzdialený prístup na školský server. Správca sa rozhodol použiť protokol SSH a každému študentovi pripravil účet s prihlasovacím menom a náhodne vygenerovaným 12 miestnym heslom. Na školskom serveri však fungujú aj iné

sieťové služby, ktoré napríklad zabezpečujú funkcionalitu webovej stránky školy. Ako by ste zabezpečili vzdialený prístup študentov tak, aby neboli ohrozené ostatné služby prístupné na serveri? Svoje tvrdenia odôvodnite:

_____

_____

_____

8. Vaša škola práve zaviedla nový jedálenský systém, ktorý umožňuje študentom a profesorom objednávať si jedlo týždeň vopred a zaplatiť zaň elektronickým kreditom. Študenti sa do tohto systému prihlasujú na webovej stránke školy pomocou svojho identifikačného čísla a zvoleného hesla. Ako by ste zabránili úniku hesiel?

_____

_____

_____

9. Na Internete existuje veľké množstvo webových portálov, ktoré umožňujú svojim návštevníkom sledovať televízne seriály online, bez toho, aby museli zaplatiť poplatok. Ich hlavnou finančnou motiváciou sú však reklamy, na ktoré keď návštevník klikne, prispeje tak k finančnej odmene prevádzkovateľa. Jožko klikol na podobnú reklamu a odvtedy mu vždy po zapnutí webového prehliadača vyskakuje nasledujúca stránka (pozri priložený obrázok). Ako by ste sa zachovali na Jožkovom mieste?

_____

_____

_____

Obrázok k úlohe č. 9

Nasledujúce otázky sú náročnejšie, preto svoju odpoveď dôkladne zvážte.

10. Webový server Vašej spoločnosti dostane zrazu obrovské množstvo požiadaviek na načítanie webovej stránky. Po zrútení webového servera sa pokúsite o jeho reštartovanie. Skontrolujete aj logy webového servera, na základe ktorých zistíte, že niektoré požiadavky na webovú stránku prišli aj z Vašej siete. O aký druh útoku sa s najväčšou pravdepodobnosťou jedná?

a) rootkit b) botnet c) vírus d) červ

Zdôvodnenie svoju odpoveď:

_____

_____

_____

11. Ktorý z uvedených spôsobov predstavuje najlepšiu možnosť ako sa brániť pred červom?

a) antivírusové skeny
b) včasné softvérové záplaty
c) vzdelávacie programy
d) správna konfigurácia firewallu

Zdôvodnenie svoju odpoveď:

_____

_____

_____

12. Vašou úlohou je vykonať posúdenie zabezpečenia Webového servera vo vašej spoločnosti a identifikovať chybný skript. Aké odporúčania poskytnete Vašej spoločnosti? Vyberte jednu:

a) Používatelia webových stránok by podľa Vás mali zakázať používanie Java appletu v rámci svojho webového prehliadača.
b) Poradím používateľom webových stránok, aby cookies prenášali len cez zabezpečené pripojenia.
c) Používatelia by mali zakázať podporu ActiveX v rámci svojich webových prehliadačov
d) Poradíte správcom webového servera, aby všetky verejné dátové vstupy boli overené pred ich spracovaním.

Zdôvodnenie svoju odpoveď:

_____

_____

_____

Príloha C

SSH SERVER A NCRACK
(prvá časť)

1.) Importujte si operačný systém do VirtualBoxu. Predchádzajúcu verziu vymažte. Počas importovania nezabudnite reinicalizovať MAC adresu všetkých sieťových kariet virtuálneho stroja. Prečo je dôležité spraviť tento krok?

_____

_____

2.) Po spustení virtuálneho stroja sa prihláste pod prihlasovacím menom *student* a heslom *studentpasswd*. Otvorte terminál a zmeňte heslo tak, že si ho neskôr budete pamätať. Použite príkaz *passwd*. Jeho vysvetlenie nájdete v slovníku pojmov na webovej stránke skoly.upjs.sk/aktivity. Nezabudnite pri zmene hesla najskôr zadať svoje aktuálne heslo! Heslo nikdy nemeňte pod používateľom root! Tento virtuálny stroj ešte budeme potrebovať :-)

3.) Zistite **IP ADRESU** vášho virtuálneho zariadenia :_____.
Vymeňte si ju so svojím susedom: _____.

4.) Prihláste sa na virtuálne zariadenie Vášho suseda, pomocou príkazu *ssh student@ipadresa – p 6666.* Požiadajte od svojho spolužiaka heslo, ktoré zadal v úlohe č. 2. Prihláste sa a pomocou príkazu *mkdir názov* mu vytvorte priečinok v domovskom adresári. Časti príkazu, ktoré sú podčiarknuté musíte nahradiť reálnymi hodnotami. Požiadajte spolužiaka, aby skontroloval, či sa Vami vytvorený priečinok skutočne nachádza v jeho virtuálnom zariadení. Čo znamená parameter príkazu -p? Nezabudnite sa potom odhlásiť z virtuálneho zariadenia Vášho spolužiaka.

_____

_____

5.) OpenSSH server je zvyčajne hneď po inštalácii spustený na porte 22. Aký súbor musíme editovať, aby sme zmenili číslo portu? Napíšte jeho absolútnu adresu: _____ .

Zakrúžkujte možnosti, ktoré budete potrebovať na zmenu portu:

nano editor	IP adresu Vášho spolužiaka
MAC adresu Vášho spolužiaka	heslo na účet root

6.) Ak sa vám podarí úspešne editovať konfiguračný súbor, bude potrebné reštartovať SSH server. Nájdite v prezentácii príkazy, ktoré to umožňujú a reštartujte server. Nezabudnite sa prihlásiť ako root.
Použité príkazy: _____.

7.) Teraz, keď ste už zmenili číslo portu na číslo 22, budete potrebovať parameter -p pri zadávaní prihlasovacieho príkazu? Podčiarknite áno alebo nie.

ÁNO / NIE

8.) Preskenujte sieť svojho spolužiaka prostredníctvom nástroja nmap. Do terminálu stačí napísať príkaz *nmap ipadresa*. Aké čísla ste našli? Napíšte ich do pracovného listu :

9.) Navštívte priečinok ***/usr/local/share/ncrack/*** a pozrite sa, aké súbory obsahuje. Zobrazte alebo otvorte v editore nano súbor **top50000. pwd** a zapíšte doňho kdesi na začiatok heslo Vášho spolužiaka. Môžete aj presvedčiť spolužiaka, aby si vybral jedno zo slov ako svoje prihlasovacie heslo. Ako by ste charakterizovali heslá uložené v tomto súbore? Čo sa Vám na nich nezdá?

_____

_____

_____

10.) Použite nástroj ncrack na odhalenie hesla používateľa:
ncrack -p číslo Portu -v -u menoPoužívaeľa -P názovSlovníka Ipadresa
Podarilo sa Vám odhaliť heslo? Ako dlho to trvalo?

11.) Pokúste sa na Inernete vyhľadať nástroje, ktoré umožňujú rovnakú činnosť ako ncrack. Ich názvy si zapíšte do pracovného listu:

_____

_____

SSH SERVER A KIPPO HONEYPOT
(druhá časť)

1.) Zmeňte číslo portu, na ktorom počúva SSH server na číslo rôzne od 22.

2.) Navštívte priečinok */home/kippo/hp/kippo-0.5/* a otvorte konfiguračný súbor honeypotu Kippo. Ako sa volá tento súbor? Nájdite v ňom číslo portu, na ktorom počúva honeypot Kippo.

Názov súboru: _____

Číslo portu: _____

3.) Počuli ste už o iptables? Viete na čo slúži?

_____

_____

Prihláste sa pod používateľským účtom root a zadajte do príkazového riadku tento príkaz:
*iptables -t nat -A PREROUTING -p tcp –dport **22** -j REDIRECT –to-port **portKIPPO***

4.) Pouvažujte o tom, čo sa práve udialo. Vyberte správnu možnosť:

a) reštartovali sme ssh server
b) všetky pakety smerujúce na port KIPPO sme presmerovali na port 22
c) vymazali sme MAC adresu
d) všetky pakety smerujúce na port 22 sme presmerovali na port KIPPO

5.) Prihláste sa ako používateľ *kippo* s heslom *kipopasswd*. Heslo nemeňte! Použi príkaz **su**, ale nezabudni za su napísať aj meno používateľa, na ktorého sa chcete prihlásiť!

6.) Vojdite do priečinka, v ktorom sa nachádzajú konfiguračné súbory Kippo honeypotu. Nájdite skript, pomocou ktorého spustíte honeypot. Spustíte ho volaním *sh nazovSúboru*. Potom sa odhláste z konta používateľa kippo.

7.) Poproste spolužiaka, aby sa prihlásil na váš SSH server, ale s použitím prihlasovacieho mena root a hesla 123456.
Čo sa udialo?

_____

_____

8.) Navštívte webovú stránku ://localhost/kippo-graph/ a napíšte, čo všetko viete z grafov vyčítať:

_____

_____

_____

_____

_____

9.) Predpokladajme, že sa útočníkom podarilo trafiť pomocou nástroja Ncrack vaše skutočné root heslo. Čo spravíte ako prvé?

a) Vygenerujem si nové heslo.
b) Zapnem honeypot.
c) Vypnem SSH server.
d) Vypnem PC.

Podarilo sa vám zistiť pomocou nástroja Ncrack aj root heslo?

10.) Pokúste sa zmeniť prihlasovacie údaje, ktorými sa útočník prihlasuje na Kippo honeypot. Aký súbor ste upravili?

11.) Upravte hostname honeypotu tak, aby to vyzeralo, že sa útočník dostal do dôveryhodného systému. Keby ste boli útočník, čo by vás presvedčilo, že systém nie je reálny?

12.) Na stránke kurzu Moodle si prečítajte odporúčania na zabezpečenie serveru SSH. Vyskúšajte si niektoré z týchto odporúčaní zrealizovať na Vašom vlastnom virtuálnom zariadení. Zhodnoťte pravdepodobnosť útoku po aplikovaní uvedených opatrení.

13.) Vyskúšajte si aj iné typy útokov na server SSH, napríklad brute-force útok pomocou nástroja Hydra. Porovnajte dĺžku trvania oboch útokov. Pri hľadaní útokov môžete používať Internet. Ak sa Vám podarí uskutočniť útok, popíšte ho spolužiakom na stránke Moodle kurzu v časti Diskusné fórum. Vaša aktivita bude bodovo ohodnotená!

Príloha D

Obsah DVD:

1. Honeypot Live CD – iso.
2. Zdrojové súbory webového portálu vrátane štruktúry databázy.
3. Malvér pre výučbu.
4. Dotazníky, vstupný test a pracovné listy.