VÝUČBA PREDMETU ETICKÝ HACKING NA FMUK

Vincent Karovič
Peter Veselý
Michal Greguš

Univerzita Komenského, Fakulta managementu, Bratislava

Abstrakt
Článok sa zaoberá začatím výučby predmetu s názvom Etický hacking na Fakulte managementu UK inovatívnou metódou a priblížením priebehu výučby tohto predmetu. Vzdelávanie študentov prebieha bezpečne pomocou systému virtualizačného prostredia openStack, v ktorom majú študenti možnosť skúšať a testovať informačné a operačné systémy vrátanie sietí v tzv. „sandboxe“ bez rizika interferencie a poškodenia školskej siete.

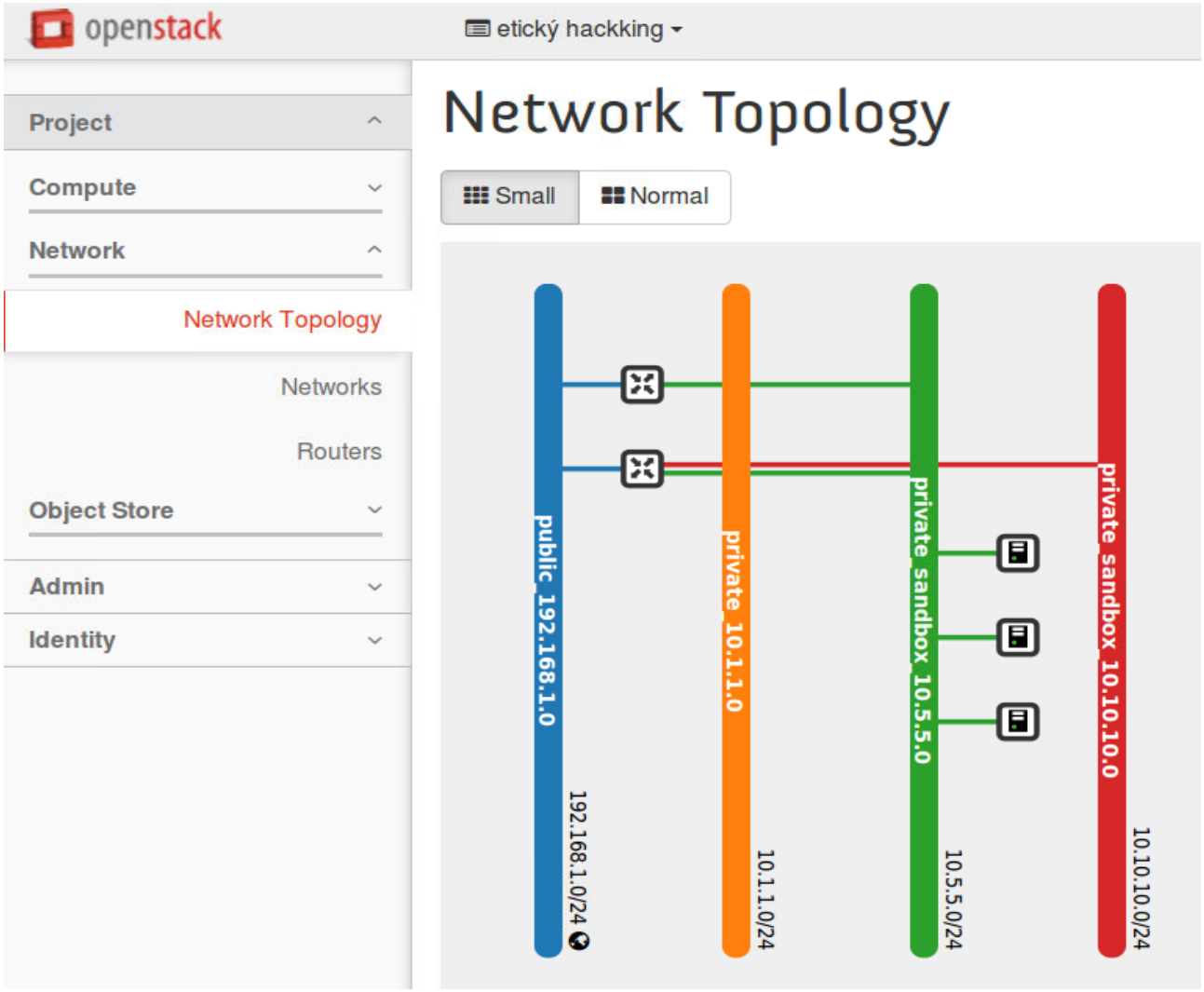
Úvod

Problematika etického hackingu je v súčasnom globalizovanom svete informačných technológii výrazným prvkom, ktorý rozhoduje o architektúre IS/ICT v podnikoch. Prakticky všetky podniky v súčasnosti spracovávajú veľmi citlivé dáta ako napr. osobné údaje, preto podľa legislatívy musia vytvoriť bezpečnostný projekt a musia sa zaoberať manažmentom bezpečnosti. Praktickou stránkou testovania bezpečnosti IS/ICT (5) vo firmách je práve etický hacking. Ide o využívanie bežne dostupných, ako aj menej dostupných techník ako sa dostať do systémov, prípadne ich poškodiť. Manažér nemôže tvrdiť, že jeho informačný systém je bezpečný, pokiaľ nespracoval komplexnú sadu bezpečnostných testov a nevyhodnotil ich z hľadiska závažnosti (2). V súčasnosti existuje medzinárodný štandard OWASP – Open Web Application Security Project (7), ktorý definuje postupné kroky, ako vykonávať dané testy. Na vykonanie týchto krokov v mene spoločnosti je však potrebný špecialista, tzv. „etický hacker“, ktorý musí disponovať dostatočnými znalosťami v tejto oblasti. Príprava týchto špecialistov vyžaduje nielen teoretické poznatky ale najmä praktické skúsenosti. V prostredí školskej siete až doteraz nebolo možné zaviesť daný predmet do výučby, respektíve realizovať praktickú časť predmetu, pretože nebol vytvorený dostatočne izolovaný systém (sandbox), ktorý by mohol slúžiť práve na simuláciu práce etického hackera. Nasledujúca časť článku bude venovaná opisu realizácie výučby predmetu Etický hacking v prostredí školskej siete.

Implementované prostredie pre výučbu

Hlavnou časťou systému pre vzdelávanie etického hackingu je virtualizačný nástroj založený na softvéri openStack (6). Systém virtualizácie spĺňa parametre pre vytvorenie prostredia, ktoré je oddelené od okolitých technológií, tzv. sandbox. Technológia umožňuje vytvoriť izolovaný

priestor siete, prípadne niekoľko sietí (viď obrázok 1), virtualizovať úložný priestor a výpočtový výkon (4).



Obrázok 1: Virtualizované siete pre predmet etický hacking

V systéme sú vytvorené rôzne bezpečnostné skupiny a virtuálny firewall pre jednotlivé virtuálne inštancie, ktorý zabezpečuje vysokú kontrolu nad prichádzajúcou a odchádzajúcou sieťovou komunikáciou. Prostredie virtualizácie sa ovláda z webového rozhrania, čo umožňuje pristupovať prakticky z ľubovoľného klientskeho počítača a je vhodné pre súbežné použitie viacerých užívateľov. Pre potreby výučby boli nainštalované v systéme openStack virtuálne servery a virtuálne pracovné stanice. Momentálne sú vytvorené servery na platforme Linux Ubuntu a v budúcnosti je v pláne doplniť aj ďalšie platformy. Na týchto serveroch sú momentálne nasadené štandardizované aplikácie ako Wordpress, ownCloud, prípadne iné vo fáze príprav (Joomla, Prestashop, Zencard, Opencard). Ako pracovná stanica určená pre etického hackera slúži distribúcia Kali Linux. Práve operačný systém Kali Linux je vyvinutý spoločnosťou, ktorá vykonáva okrem školení aj medzinárodné certifikácie etických hackerov. Systém dokáže monitorovať siete a analyzovať sieťovú komunikáciu až na úroveň fyzických paketov. (3) V priebehu výučbových hodín prebiehajú penetračné testy jednotlivých serverov s

postupným plnením krokov podľa OWASP metodiky. Študenti majú k dispozícii množstvo nástrojov a predpripravené scenáre penetračných testov.

V súčasnosti je pripravených niekoľko obrazov virtualizovaných systémov, napríklad Ubuntu server, CentOS a Kali Linux, pričom je naplánovaná aj príprava servera založeného na technológiách spoločnosti Microsoft. Obrazy operačných systémov sú zálohované zatiaľ na strane servera pre prípad poškodenia, ktoré môže nastať pri penetračných testoch. V rámci návrhu architektúry siete je pripravený model siete zo štyroch podsietí, umiestnenia serverov, pracovných staníc v nich a virtuálnych prvkov ako sú routery (openStack Neutron sieť) (1).

Obsah predmetu

Obsahom predmetu Etický hacking je objasniť zložitosť a rozsah problému zabezpečenia systémov pre spracovanie údajov a poskytovanie informácií s dôrazom na úlohu manažéra v procese budovania a prevádzkovania takýchto systémov. Úvod tvoria všeobecné základy bezpečnosti a vymedzenie pojmu „bezpečný informačný systém“. Ďalej sú rozobrané základné technické a programové prostriedky ochrany IS a špecifiká bezpečnosti v sieťach. Kľúčové sú rozdiely pre zásady bezpečnosti pri procese vzniku IS a zásady bezpečnosti pri prevádzka IS. Ľudský faktor a bezpečnostná kultúra organizácie majú napomôcť pri chápaní úlohy manažéra bezpečnosti v organizácii. Teoretické poznatky sú nakoniec zhrnuté v základných bezpečnostných princípoch. Študent sa taktiež má oboznámiť s úlohou auditu IS.
Z týchto tematických okruhov boli v predmete naplánované jednotlivé semináre ako tematický plán.

Tematický plán:

1. Úvod do etického hackingu
2. Praktická ukážka nástrojov určených pre penetračné testovanie
3. Praktická ukážka penetračného testu IT bezpečnosti servera
4. Základné princípy počítačových vírusov
5. Demonštrácia monitorovania sietí
6. Možnosti priamych útokov na sieťové zariadenia
7. Demonštrácia možnosti ochrany proti technikám hackerov
8. Personálna bezpečnosť a bezpečnosť biometrických osobných údajov
9. ISO 27001 - systém manažmentu bezpečnosti
10. Zákon č. 122/2013 Z.z. – Zákon o ochrane osobných údajov
11. OWASP - Open Web Application Security Project
13. Sociálne inžinierstvo
14. Trendy v manažmente bezpečnosti
15. Študentský battle v sandboxe

Po úspešnom absolvovaní by mali študenti ovládať základy IT bezpečnosti a mali by byť schopní testovať bezpečnosť IS/ICT vo firme, uplatňovať princípy informačnej bezpečnosti IS/IT vo svojej manažérskej praxi a aktívne pôsobiť v rámci systému riadenia informačnej bezpečnosti vo firme v rôznych fázach vývoja životného cyklu IS/IT.

Inovácia výučby

Inovácia výučby spočíva použití virtualizačného nástroja simulujúceho reálne sieťové riešenie IS/IKT. Cieľ a prínos je v získaní empirických skúseností vďaka možnosti prakticky vyskúšať techniky útočníka-hackera aj ochrancu-administrátora alebo manažéra bezpečnosti IS/IKT. Na záver semestra bola pre študentov pripravená a odskúšaná malá súťaž, tzv. „študentský battle v sandboxe“. Prvá skupina študentov má za úlohu upraviť a nastaviť zámerne zle zabezpečené technologické riešenia, ktoré boli vytvorené lektorom. Študenti majú k dispozícii komplexnú sieť s aktívnymi sieťovými prvkami a pripravenými aplikáciami, ktoré však nepripravovali oni sami. Druhá, súperiaca skupina študentov má za úlohu hľadať chyby v zabezpečení po opravách prvej skupiny. Obe skupiny študentov predmetu Etický hacking musia realizovať tzv. „black test“ podľa OWASP s nasadením systému Kali Linux. Študenti tak majú možnosť reálne otestovať svoje vedomosti a zručnosti a získať tak empirické skúsenosti s ochranou IS/ICT. Práve vďaka praktickým cvičeniam získajú predstavu o penetračných testoch a osvoja si zásady pri riadení bezpečnosti v organizácii.

Záver

V súčasnej dobe je ochrana a zabezpečenie informačného systému respektíve ochrana informácií veľmi zásadnou úlohou manažérov a to nielen v podnikovej sfére. Príprava manažérov na úlohu spojenú s ochranou informácií môže začať už na školách pomocou výučby a to nielen v teoretickej rovine (5). Predmet Etický hacking pomocou praktického cvičenia, ukážkami techník a premýšľania nad slabými miestami informačných systémov môže napomôcť budúcim manažérom pri riadení bezpečnosti toku informácií v organizáciách. Výučba predmetu bez použitia virtuálneho prostredia openStack bola veľmi náročnou úlohou a väčšina ukážok techník a nástrojov nebolo možné realizovať, vzhľadom na zabezpečenie školskej siete. Použitím softvéru openStack bolo dosiahnuté oddelenie systému zabezpečujúceho chod školy a výukového – testovacieho prostredia, v ktorom bolo možné rýchle nasadenie rôznych modelov a testovanie ich bezpečnosti. Najdôležitejším parametrom bolo zabezpečenie oddelenia kritických častí školskej siete od modelov sieti a technológií tvorených vo virtuálnom prostredí openStacku, avšak so zabezpečením prístupu do internetu, čím sme dosiahli, že sa systém javil ako reálny. Prostredie bolo testované jeden semester a výučba prebehla s ohľadom možnosti servera a prispôsobené na jeho funkcionality. Plán

budúcej výučby predmetu je orientovaný na zavedenie hybridnej architektúry a testovanie aj iných systémov a architektúr siete.

Referencie

1. DRAHOŠOVÁ, M. a KAROVIČ, V., 2015a. Cloud and virtualization in Linux environment. V: *CER Comparative European research 2015 : International Scientific Conference for PhD students of EU countries [4th] - London* [online]. s. 130–133. ISBN ISBN 978-0-9928772-8-6. Dostupné na: http://www.sciemcee.org/library/proceedings/cer/cer2015_proceedings02.pdf

2. DRAHOŠOVÁ, M. a KAROVIČ, V., 2015b. Information security. V: *CER Comparative European research 2015 : International Scientific Conference for PhD students of EU countries [4th] - London* [online]. s. 134–137. ISBN ISBN 978-0-9928772-8-6. Dostupné na: http://www.sciemcee.org/library/proceedings/cer/cer2015_proceedings02.pdf

3. KAROVIČ, V., 2013. Linux. *Digital Science Magazine* [online]. 2013 [cit. 29. apríl 2016]. ISSN ISSN 1339-3782. Dostupné na: http://digitalmag.sk/linux/

4. KAROVIČ, Vincent, Vincent KAROVIČ, Peter VESELÝ, František OLŠAVSKÝ a Michal GREGUŠ, 2016. Nasadenie virtualizačného prostredia openstack na výučbové účely. *Marketing science and inspirations*. 2016, s. 43–52. ISSN 1338-7944.

5. MUČKOVÁ, O., KAROVIČ, V. a KRAJČÍK, M., 2015. Bezpečnosť ako jeden z prvkov integrovaného systému manažérstva. *Digital Science Magazine* [online]. 2015. ISSN ISSN 1339-3782. Dostupné na: http://digitalmag.sk/bezpecnost_ako_jeden_z_prvkov/

6. OPENSTACK, 2016. *OpenStack Docs: Overview and components* [online] [cit. 13. október 2016]. Dostupné na: http://docs.openstack.org/liberty/networking-guide/intro-os-networking-overview.html

7. OWASP, 2016. *OWASP* [online] [cit. 13. október 2016]. Dostupné na: https://www.owasp.org/index.php/Main_Page