Slovenská technická univerzita v Bratislave

Fakulta informatiky a informačných technológií

Študijný odbor: Počítačové Systémy a Siete

Ponuka produktu

Penetračné testovanie

Tímový projekt

Vedúci projektu: Doc. Ing. Ladislav Hudec, CSc.; Ing. Adrian Bagala

Borlok Ján	jan.borlok@allenovery.com
Krištof Ján	deity@pobox.sk
Kubík Matej	kubik@zuikaku.org
Lenz Roman	nolimits@pobox.sk
Mateja Miroslav	hooki@r3.roburnet.sk

Obsah

1 Úvod

Bezpečnosť počítačov a počítačových sietí je dnes často skloňovaným pojmom. Je to celkom pochopiteľné, pretože neoprávnená osoba, ktorá prenikne do počítačovej siete spoločnosti (napríklad firmy), môže spôsobiť veľmi veľké škody, či už priame alebo nepriame. Jednou z dôležitých častí počítačovej bezpečnosti je takzvaná sieťová bezpečnosť, ktorá sa zaoberá ochranou pred útokmi prichádzajúcimi cez počítačovú sieť. Jeden z najčastejšie používaných prvkov sieťovej bezpečnosti je takzvaná bezpečnostná brána, ktorá chráni privátnu časť siete pred útokmi s verejnej siete.

Na udržanie primeranej bezpečnosti brány pred vonkajšími útokmi je nutné jej opakované testovanie. Jedným z možných prístupov k tomuto testovaniu je takzvané penetračné testovanie, ktoré napodobňuje správanie sa útočníka pri útoku (pokuse o penetráciu) na systém.

2 Členovia tímu

Tím bol vytvorený na začiatku semestra a má päť členov (v abecednom poradí):

Bc. Borlok Ján	jan.borlok@allenovery.com
Bc. Krištof Ján	deity@pobox.sk
Bc. Kubík Matej	kubik@zuikaku.org
Bc. Lenz Roman	nolimits@pobox.sk
Bc. Mateja Miroslav	hooki@r3.roburnet.sk

Zloženie nášho tímu je veľmi rôznorodé. Všetci členovia ukončili bakalárske štúdium v odbore Počítačové Systémy a Siete na Fakulte Informatiky a Informačných Technológií Slovenskej Technickej Univerzity v Bratislave. Každý člen tímu má za sebou dlhodobú prax v študovanom odbore, čo považujeme za jednu z výhod nášho tímu.

Charakteristiky jednotlivých členov tímu sú uvedené v nasledujúcej časti tejto kapitoly.

- ***Bc. Borlok Ján***

  Je absolventom bakalárskeho štúdia na FIIT STU v Bratislave v odbore Informatika, špecializácia Počítačové systémy a siete a študentom inžinierskeho štúdia na FIIT STU v rovnakom odbore. Má úspešne absolvované všetky 4 semestre CCNA a momentálne sa pripravuje na certifikáciu. Pri štúdiu získal bohaté skúsenosti s programovaním v rôznych vývojových aplikáciách za ktoré možno spomenúť C++. Vo voľnom čase rád vytvára HTML prezentácie za pomoci PHP a SQL.

  Okrem štúdia má bohaté skúsenosti z praxe. Viac ako 4 roky je zamestnaný ako správca site. Medzi nadobudnuté skúseností patrí administrácia Windows serverov a ich zabezpečenie, implementácia PKI a zabezpečenie bezdrôtových

sietí. Medzi nezanedbateľné skúsenosti patrí určite implementácia internetových bezpečnostných brán a proxy serverov.

- ***Bc. Krištof Ján***

Je absolventom bakalárskeho štúdia na FIIT STU v Bratislave v odbore Informatika, špecializácia Počítačové systémy a siete a študentom inžinierskeho štúdia na FIIT v rovnakom odbore. Má skúsenosti s programovaním v jazykoch C, C++.

Vlastní certifikát 1. až 4. semestra kurzu Cisco Certified Network Associate (CCNA). Tiež sa tu zoznámil s konfigurovaním CISCO zariadení (routre, switche) a štruktúrou ich hardvéru a operačného systému.

Skúsenosti s prácou v tíme získal prácou v súkromnej firme.

- ***Bc. Kubík Matej***

Je absolventom bakalárskeho štúdia na FIIT STU v Bratislave v odbore Informatika, špecializácia Počítačové systémy a siete a študentom inžinierskeho štúdia na FIIT v rovnakom odbore. V záverečnej práci bakalárskeho štúdia spracovával projekt Penetračné testovanie, v ktorom si prehĺbil svoje znalosti z bezpečnosti počítačových systémov.

Popri štúdiu bol zamestnaný 2 roky na FTVŠ UK ako správca počítačovej siete, neskôr 3 roky vo firme NetlabPlus, ktorá sa zaoberá poskytovaním Internetu a dátových liniek, ako operátor. Tam sa podieľal na udržiavaní v prevádzke a chránení počítačovej siete slúžiacej stovkám zákazníkov. Okrem toho sa v tejto firme zaoberal vývojom operačného systému pre embedded smerovače na báze FreeBSD, systému na monitorovanie funkčnosti siete a programovaním systémových utilít v jazykoch C a Perl. Okrem popísaných má skúsenosti aj s vývojom aplikácií pre databázové prostredie PostgreSQL.

Počas svojej praxe získal skúsenosti s prácou samostatne i v tíme na väčších aj menších projektoch.

- ***Bc. Lenz Roman***

Je absolventom bakalárskeho štúdia na FIIT STU v Bratislave v odbore Informatika – Počítačové systémy a siete. Má skúsenosti s programovaním v jazykoch C, C++, Pascal/Delphi, PHP, HTML. Počas štúdia získal bohaté skúsenosti s návrhom a vývojom aplikácií pre platformu Win32 (v prostredí MS Visual C++), ale má aj skúsenosti s programovaním na platforme UNIX (Linux, BSD).

Absolvoval kurzy CCNA 1 – 3, kde získal podrobné informácie o stavbe a fungovaní počítačových sietí. Tiež sa tu zoznámil s konfigurovaním CISCO zariadení (routre, switche) a štruktúrou ich hardvéru a operačného systému.

Skúsenosti s prácou v tíme získal prácou v súkromnej firme.

- ***Bc. Mateja Miroslav***

Venuje sa informačným technológiám už od útleho veku. Nazbieral množstvo skúseností v rôznorodej škále programovacích jazykov. Je absolventom bakalárskeho štúdia na FIIT STU v Bratislave v odbore Počítačové systémy a siete. Má veľmi dobre znalosti a skúsenosti s programovaním v C, C++ vo vývojovom prostredí Visual C++, ale špecializuje sa na programovanie web aplikácii a ich bezpečnosť. Ovláda HTML, XHTML, PHP, JavaScript, veľmi dobre SQL. Základné znalosti má aj z Flash ActionScriptu, LUA scriptu a unixového C shellu, ktoré si v súčasnej dobe prehlbuje samoštúdiom.

Momentálne robí v programovacej firme špecializujúcej sa na návrh a vývoj web-portálových riešení, kde pracuje s ďalšími programovacími jazykmi ako XML, XSL, JSP a Javou. Vo voľnom čase sa venuje obohacovaniu svojich vedomostí rôznymi kurzami ako napríklad CCNA, kde má zatiaľ absolvovaný prvý semester. Nebráni sa pre neho novým veciam ba má priam na ne apetít.

3 Motivácia

Výber témy tímového projektu bol ovplyvnený niekoľkými faktormi:

Všetci sme študentmi zamerania Počítačové Systémy a Siete, ku ktorému je tento projekt najbližšie. Takisto sme počas štúdia absolvovali viacero predmetov a kurzov, ktoré nás dostatočne teoreticky ale aj prakticky pripravili na takýto druh projektu a nadobudli sme potrebné znalosti na jeho úspešné vyriešenie.

Samotná teória samozrejme nestačí. Každý člen nášho tímu už pracuje čím si svoje teoretické znalosti priamo overuje v skutočnej praxi. V tomto projekte, by sme si chceli ďalej prehĺbiť naše schopnosti riešiť zadania spoločne ako tím.

Nadchla nás možnosť vytvoriť použiteľný produkt pre testovanie bezpečnostných slabín počítačových systémov a tiež pocit, že existuje šanca vytvoriť niečo, čo sa môže nasadiť do reálnej prevádzky a poprípade neskôr presadiť v konkurencii.

4 Čo môžeme poskytnúť

Naše riešenie systému pre penetračné testovanie bude spĺňať požiadavky stanovené zadaním a bude sa skladať z dvoch častí. Prvou časťou bude Webová stránka demonštrujúca princípy penetračného testovania a popisujúca voľne dostupné nástroje na penetračné testovanie ako napr. Nessus, NetSAINT či SARA. Druhou časťou bude integračné prostredie pre penetračné testy. To bude používať bázu znalostí o testovanom systéme, pomocou ktorej bude riadiť priebeh testovania.

Užívateľské rozhranie bude nezávislé na testovacom jadre a bude s ním komunikovať jedným spojením, aby mohlo bežať aj na inom sieťovom uzle ako jadro. Malo by poskytovať nasledujúce funkcie:

- zadanie informácií nutných na spojenie s jadrom a informácie o stave spojenia s jadrom,
- informácie o skupinách skriptov a limitácia spúšťaných skupín; skupiny sa budú deliť jednak podľa ohrozenia funkčnosti testovaného uzlu (žiadna, dočasné zahltenie služby, odstávka služby do zásahu administrátora, odstávka uzlu do zásahu administrátora a pod.) a podľa oblasti testovania,
- zadanie testovaného uzlu a spustenie testovania,
- monitorovanie priebehu testovania,
- informácie o výsledkoch testu a bezpečnostných chybách na testovanom uzle; informácie o chybách by mali byť súčasťou skriptu, ktorý príslušnú chybu testuje.

Báza znalostí a závislostí popisuje, aké vedomosti o testovanom systéme tester má. Dynamicky ju vytvára a udržuje samotný testovací stroj na základe informácií zo skriptov:

- aké znalosti sú na beh skriptu potrebné (napr. nie je možné testovať verziu HTTP servera, ak nevieme, na akom porte počúva),
- aké znalosti sa so skriptom vylučujú (napr. nemá zmysel testovať zraniteľnosť týkajúcu sa zariadení Cisco, ak sme zistili, že na systéme beží OS Windows),
- aké znalosti skript pri svojom behu získa.

Báza znalostí môže obsahovať napríklad nasledujúce informácie pre každý port:

- či je obsluhovaný,
- aká služba na ňom beží (HTTP, SMTP, SNMP...),
- typ a verziu obslužného procesu (IIS, Apache...), a pre každý testovaný uzol:
    - typ a verziu OS alebo zariadenia,
    - či je možné vykonávať testy, ktoré môžu narušiť funkčnosť systému.

Tvorba testovacích skriptov nie je súčasťou tohoto projektu, napriek tomu je však nutné vytvoriť niekoľko skriptov na základné testovanie a pre referenciu. Testovacie skripty sa budú skladať z dvoch častí:

- popis vzťahu skriptu k báze znalostí,
- informácie, do akých skupín sa skript radí,
- samotné telo skriptu.

Programovací jazyk a prostredie, v ktorom sa budú testovacie skripty vytvárať, bude určené v neskoršej fáze. To bude umožnené relatívnou nezávislosťou kódu skriptov na jadre.

Samotné testovacie jadro bude zabezpečovať:

- komunikáciu s užívateľským rozhraním, príjem príkazov a výpis správ o testovaní,
- analýzu informácií o testovacích skriptoch a tvorbu bázy znalostí podľa ich pokynov,
- udržiavanie bázy znalostí,
- výber informácií z bázy znalostí, ktoré sú dôležité pre užívateľské správy, napríklad zraniteľnosti jednotlivých služieb,
- spúšťanie testovacích skriptov podľa informácií z bázy znalostí.

Jadro bude napísané v jazyku C tak, aby bolo nezávislé na testovacích skriptoch, ktoré môžu byť v ľubovoľnom jazyku.

5 Záver

V priebehu dvoch semestrov plánujeme vytvorenie systému pre penetračné testovanie, ktorý bude spĺňať všetky požiadavky kladené na tento systém.

Riešenie projektu bude prebiehať v niekoľkých fázach. Tieto vyplývajú z použitia inžinierskeho prístupu pri riešení projektu. V prvej fáze vytvoríme komplexnú analýzu používaných systémov. V druhej fáze prebehne samotná implementácia projektu.

Tento dokument obsahuje ponuku na systém na podporu penetračného testovanie. Náš tím s rozsiahlymi skúsenosťami s technológiami používanými v prostredí internetu je vhodný na tvorbu práve takéhoto systému. Motivácia nášho tímu s tým čo môžeme poskytnúť sú dôkazom našej schopnosti vytvoriť systém ako užitočnú pomôcku pre overenie zabezpečenia systému.

6 Odkazy

[1] The Nessus Project: www.nessus.org
[2] Security Administrator Tool for Analyzing Networks: www.fish.com/satan/
[3] GULA, R.: Broadening the Scope of Penetration-Testing Techniques. Enterasys Networks, Inc., 2001.
http://www.enterasys.com/products/whitepapers/security/9012542.pdf
[4] HERZOG, P. et al.: Open Source Security Testing Methodology Manual. 2003.
http://www.osstmm.org/

Príloha 1: Priorita tém

1. Penetračné testovanie
2. Multimediálna podpora predmetu Architektúra počítačov
3. Virtuálna univerzita
4. Simulátor komunikácie v počítačovej sieti

Príloha 2: Rozvrh členov tímu

		7:20	8:15	9:15	10:10	11:10	12:05	13:05	14:00	15:00	15:55	16:55	17:50	18:50	19:50	20:45
Pondelok	JB															
	JK															
	MK															
	RL															
	MM															
Utorok	JB															
	JK															
	MK															
	RL															
	MM															
Streda	JB															
	JK															
	MK															
	RL															
	MM															
Štvrtok	JB															
	JK															
	MK															
	RL															
	MM															
Piatok	JB															
	JK															
	MK															
	RL															
	MM															

JB - Borlok Ján
JK - Krištof Ján
MK - Kubík Matej
RL - Lenz Roman
MM -Mateia Miroslav

označenie vyučovacích hodín jednotlivých študentov
označenie preferovaného času pre prácu na tímovom projekte