Praktické testování do posledních detailů

Matúš Selecký

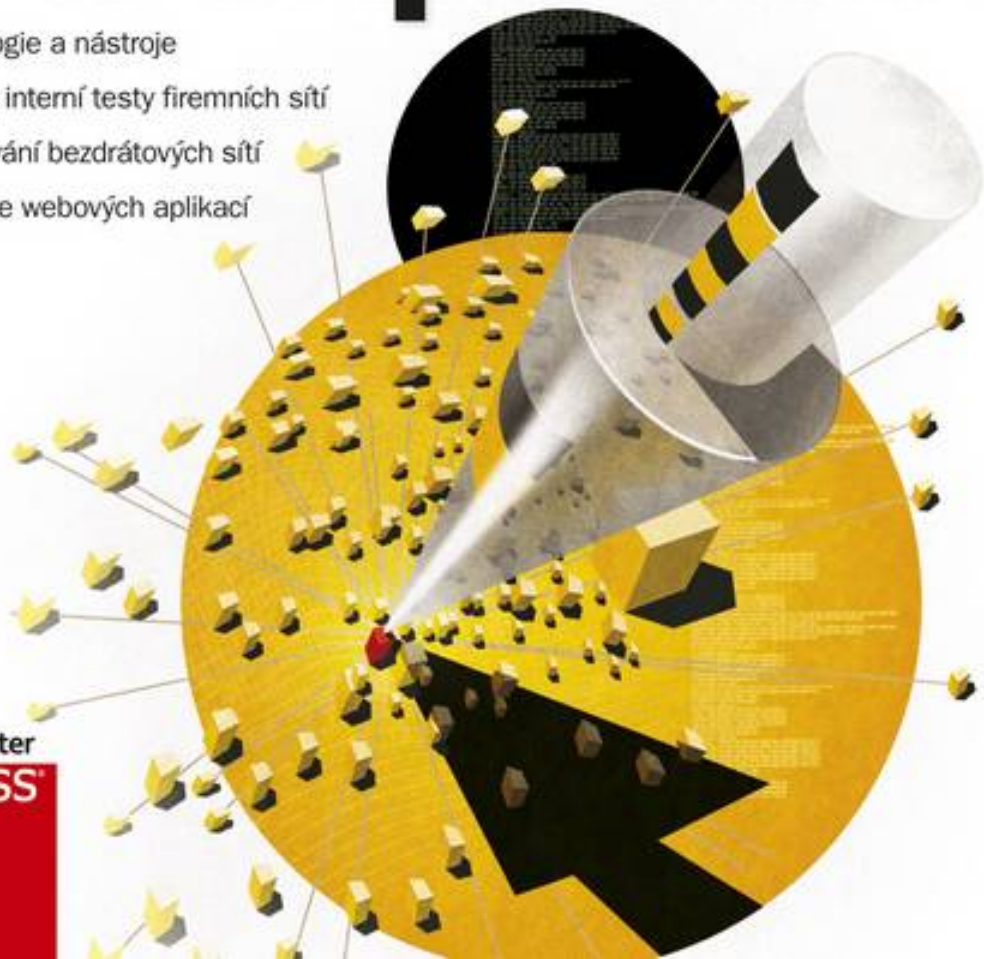
Penetrační testy a exploitace

Metodologie a nástroje

Externí a interní testy firemních sítí

Prolamování bezdrátových sítí

Penetrace webových aplikací



computer press

Matúš Selecký

Penetrační testy a exploitace

Computer Press
Brno
2012

Penetrační testy a exploitace

Matúš Selecký

Obálka: Martin Sodomka
Odpovědný redaktor: Libor Pácl
Technický redaktor: Jiří Matoušek

Objednávky knih:
http://knihy.cpress.cz
www.albatrosmedia.cz
eshop@albatrosmedia.cz
bezplatná linka 800 555 513
ISBN 978-80-251-3752-9

Vydalo nakladatelství Computer Press v Brně roku 2012 ve společnosti Albatros Media a. s.
se sídlem Na Pankráci 30, Praha 4. Číslo publikace 16 389.

1. vydání

ALBATROS MEDIA a.s.

Obsah

KAPITOLA 5

Předmluva autora

Záměrem autora bylo odlišit knihu zaměřenou na penetrační testování od ostatních knih, které jsou ohledně této tematiky dostupné na českém a zahraničním trhu. Vzhledem k rozsáhlosti probírané problematiky penetračního testování není možný popis jednotlivých částí od úplných základů do posledních detailů. Proto jsou v textu představeny pouze aplikace, které lze využít pro testování různých oblastí. Ke každé probírané aplikaci je popsáno základní použití a ukázán jednoduchý demonstrativní test s výpisem.

Aby čtenář nezůstal ochuzen o ostatní detaily, snažil se autor poskytnout velké množství odkazů, kde je možné najít další, detailnější informace.

Vzhledem k dynamickému vývoji IT oboru bylo cílem autora vytvořit dílo, které by nabízelo základní přehled a informace z oblasti penetračního testování i o několik let později.

Tímto směrem (dalšího individuálního vzdělávání) se ubírá také část první kapitoly, kde se projevuje snaha ukázat možnosti, jak a kde získávat kvalitní informace z oblasti informačních technologií s konkrétnějším zaměřením na bezpečnost.

Na tomto místě by autor rád poděkoval šéfredaktorovi nakladatelství Computer Press Liboru Páclovi.

Co obsahuje tato kniha

Kniha je rozdělena do pěti kapitol s následujícími názvy a obsahem:

1. kapitola: **Metodologie a nástroje penetračních testů** – První kapitola knihy obsahuje úvod do problematiky penetračního testování. Má za cíl objasnit jednotlivé aspekty penetračních testů a nabídnout odpovědi na několik základních otázek. Dále se pak věnuje zdrojům informací pro rozšiřování obzorů.

2. kapitola: **Externí penetrační testy firemních sítí** – Druhá kapitola se zabývá externími penetračními testy. Jedná se o testy, které ověřují bezpečnost z vnější strany firemní sítě. V úvodu je poměrně podrobně představena metodika přístupu k tvorbě a návrhů testů a cílů, na které by tyto testy měly být zaměřeny. V kapitole jsou probírány také testy síťových zařízení – přepínačů a směrovačů.

3. kapitola: **Interní penetrační testy firemních sítí** – Tato kapitola je věnována penetračním testům firemních sítí z vnitřní strany. V kapitole jsou probírány oblasti fyzické a softwarové ochrany sítě, problematika bezpečnosti hesel, sdílení dat a přístupových práv k souborům. Součástí kapitoly jsou další nástroje a testy pro testování síťových zařízení firemní infrastruktury.

4. kapitola: **Penetrační testy bezdrátových sítí** – Předposlední kapitola se zabývá problematikou penetračního testování bezdrátových sítí. Kapitola je rozdělena do dvou částí, přičemž jeden pohled je opět z vnější strany sítě, tzn. že se popisují techniky získávání informací o dané síti či možnosti a techniky prolamování zabezpečení sítě. Druhý pohled je z vnitřní strany sítě a v jeho rámci jsou probírány aspekty bezpečnosti klientských zařízení a síťových prvků.

5. kapitola: **Penetrační testy webových aplikací** – Poslední kapitola knihy je věnována problematice penetračního testování webových aplikací. Jsou zde představena zranitelná místa, která se objevovala v roce 2010 nejčastěji. V textu jsou popsány základní principy, jak se dané zranitelné místo zneužívá, a několik aplikací, s nimiž lze webovou aplikaci na přítomnost konkrétního zranitelného místa otestovat.

Jednotlivé kapitoly mají podobnou strukturu, která vychází z obecné metodiky vytvořené pro penetrační testování. Metodika a obsah jednotlivých struktur jsou blíže popsány v úvodní kapitole. Pro lepší pochopení textu je ale nezbytné blíže představit použitou schematiku textu. V dalším textu knihy budou používány následující prvky:

Webové odkazy

V jednotlivých testech, které budou v knize popisovány a v nichž se používá nějaká aplikace nebo nástroj, je uvedena webová adresa, odkud je možné stáhnout vše potřebné pro provedení testu. Adresa bývá označena následovně:

Web: `http://ip-check.info/?lang=en`

Odkazovník

Na konci některých testů je uveden odkazovník, který obsahuje odkazy a tipy na vyhledávací výrazy pro vyhledávač Google; dále odkazy a tipy na vyhledávací výrazy pro videa na videoserverech, jako je Youtube nebo Vimeo, a další zajímavé webové odkazy. V odkazovníku uvádíme také kód, pod kterým je možné najít odkaz k dané problematice v referencích na konci kapitoly.

Obecná logika je následující:

- V levém sloupci je webový server, který lze použít pro vyhledávání.
- V pravém sloupci je tip na vyhledávací výraz nebo přímo URL odkaz.
- Poslední případ v níže uvedeném příkladu odkazovníku představuje odkaz na reference na konci kapitoly.

Popisovaný odkazovník může mít například následující podobu:

Odkazovník:

Google	Android penetration testing
Books.google.com	Investigating Wireless devices
Youtube	Android penetrate, Android Security
Vimeo	`http://vimeo.com/31994652`
Web	`http://elinux.org/Android_Portal`
	`http://elinux.org/Android_Testing`
Reference	3

Výpis zdrojového kódu

V textu je u většiny použitých aplikací popisováno přesné znění příkazů, které byly použity pro provedení daného testu, a výpis, jejž vrací aplikace po provedení zadaného příkazu. To vše je označeno tímto typem písma:

```
# ncat_config
ncat_config: Reading /usr/etc/ncat.conf.MASTER
```

Očekávaný výsledek

Na konci každého testu je stručně popsáno, co můžeme od provedeného testu očekávat.

Zpětná vazba od čtenářů

Nakladatelství a vydavatelství Computer Press stojí o zpětnou vazbu a bude na vaše podněty a dotazy reagovat. Můžete se obrátit na následující adresy:

Computer Press
Albatros Media, a. s., pobočka Brno
IBC
Příkop 4
602 00 Brno

nebo

`sefredaktor.pc@albatrosmedia.cz`

Computer Press neposkytuje rady ani jakýkoliv servis pro aplikace třetích stran. Pokud budete mít dotaz k programu, obraťte se prosím na jeho tvůrce.

Errata

Přestože jsme udělali maximum pro to, abychom zajistili přesnost a správnost obsahu, chybám se úplně vyhnout nelze. Pokud v některé z našich knih najdete chybu, ať už v textu nebo v kódu, budeme rádi, pokud nám o ní dáte vědět. Ostatní uživatele tak můžete ušetřit frustrace a nám pomůžete zlepšit následující vydání této knihy.

Veškerá existující errata zobrazíte na adrese `http://knihy.cpress.cz/K2022` po klepnutí na odkaz Soubory ke stažení.

KAPITOLA 1

Metodologie a nástroje penetračních testů

V této kapitole se dozvíte:
- Úvod
- Metodologie testování
- Penetrační testování
- Vzdělávání a trénink

Úvod

V první kapitole této knihy bude pojednáváno o základech problematiky penetračního testování. Nejdříve bude popsána struktura knihy a vysvětlena metodologie, ze které kniha vychází, a na ni naváže popis penetračního testování, způsobu, jakým probíhá; probereme také technické, administrativní, právní a ekonomické aspekty penetračních testů.

V druhé části kapitoly uvedeme několik testovacích prostředí, přičemž některá budou dále používána v průběhu knihy, a několik zajímavých odkazů, jež mohou mít pro uživatele značnou informační hodnotu. Cílem je také ukázat možnosti, kde získávat nové znalosti z oblasti IT bezpečnosti.

Záměrem první kapitoly je nabídnout odpovědi na základní otázky:

- Proč jsou penetrační testy důležité?
- Co by mělo být podrobeno penetračnímu testování?
- Jaké typy penetračních testů existují?
- Jak by měly probíhat penetrační testy?
- Jaká jsou rizika penetračních testů?
- Do jaké míry je potřeba testovat?
- Jakými nástroji testovat?
- Kde najít další informace a dozvědět se více?

Metodologie testování

Při tvorbě knihy jsme se snažili vycházet z obecných metodik pro penetrační testování. Tyto metodiky nejsou vždy úplně jednotné, ale základní struktura je vždy stejná. Různé zdroje uvádějí upravené metodiky podle vlastních zkušeností, představ a požadavků. Počet jednotlivých fází testovacích cyklů se pohybuje od čtyř do sedmi. Pro účely této knihy byla zvolena a upravena metodika, která zahrnuje celkově čtyři kroky. Každá kapitola knihy proto obsahuje kromě úvodu a závěru také tyto čtyři fáze:

- Fáze 1: Cíl a rozsah penetračního testu
- Fáze 2: Sběr dat
- Fáze 3: Skenování a exploitace
- Fáze 4: Report

Nyní blíže popíšeme, co zastřešují jednotlivé fáze testovací procedury.

Fáze 1: Cíl a rozsah penetračních testů

Tato fáze slouží k tomu, aby se na základě obecných zadání a cílů určily detailnější cíle, na které budou následně zaměřeny prováděné penetrační testy. Hlavní je vymezit cíle prioritní – z praktického hlediska totiž ani není možné ověřit vše na 100 %.

Uvedená potřeba bližší specifikace a optimalizace zadaných cílů nastane, když například přijde požadavek otestovat bezpečnost konkrétní webové aplikace. Z tohoto obecného požadavku je nutné určit, co především je potřeba otestovat. Má být například otestována bezpečnost přihlašování? Bezpečnost uživatelských transakcí? Má být ověřeno zabezpečení přístupu ke konfiguracím aplikace a k informacím o uživatelích? Má se ověřovat stabilita aplikace?

Takových cílů a bodů, které mají být otestovány, může být několik. Proto je třeba v této fázi určit, co všechno se požaduje a na co je nutné se zaměřit.

Fáze 2: Sběr dat

Na základě výstupu z fáze 1 je potřeba zjistit o konkrétních systémech co nejvíce informací. Podle zvoleného typu testů (black-box, white-box, grey-box) je možné postupovat několika způsoby. Jak bude popsáno dále, každý typ testů má určité výhody a nevýhody. Táto fáze má za cíl vytvořit obraz o tom, jak a kde hledat informace o testovaném systému, případně aplikaci.

Informace se následně používají jako vstup do další fáze. Když se má například otestovat bezpečnost webové aplikace nebo webového serveru, může být jedním z procesů druhé fáze vzdálené aktivní skenování adresářové struktury. Tím lze například zjistit logickou strukturu adresářů na serveru, a v některých případech i testované webové aplikace.

Skenování je možné realizovat prostřednictvím aplikace, která dokáže vytvořit tzv. zrcadlovou kopii serveru. Kopii lze následně pasivně prohlížet a analyzovat. Tak je možné zjistit, že

do složky \XYZ ukládá aplikace informace o nabízených produktech, do složky \ABC ukládá informace o uživatelských účtech atd.

Sběr informací se může dále týkat například spřízněných společností, uživatelských e-mailových účtů, telefonních čísel, typu používaných zařízení a operačních systémů a mnoha dalších informací.

Fáze 3: Skenování a exploitace

Třetí fáze obnáší proces skenování testovaného systému, testování zabezpečení a pokusy o prolomení bezpečnostních mechanismů. Hlavním cílem exploitace může být například získání přístupu do systému nebo databáze bez validních přihlašovacích údajů, získání citlivých informací o uživatelích nebo například znepřístupnění služby.

V oblasti informačních technologií neexistuje produkt, který by byl 100% dokonalý. Vždy se vyskytne nějaký problém, který nebyl dosud odhalen. Totéž by se dalo říct o bezpečnostních prvcích používaných v různých oblastech. Jestliže zatím nedošlo k prolomení určitého bezpečnostního mechanismu, ještě to neznamená, že je tento mechanismus neprolomitelný navždy. S vývojem poznatků a znalostí může dojít k objevení nových bezpečnostních chyb a postupů, jak tyto chyby využít, čehož jsme na Internetu svědkem téměř denně.

Celý proces prolamování bezpečnostních mechanismů je postaven na využívání chyb a nedostatků v aplikacích a systémech. Častou příčinou vzniku chyb je právě časový tlak a nedostatek prostředků (zejména finančních) při vývoji a realizaci řešení. V dnešní době je možné tento tlak registrovat denně a téměř u všech podnikatelských subjektů.

Tato fáze může obecně využívat nespočetné množství postupů a přístupů, testovacích aplikací a nástrojů. Technicky není možné pokrýt celou probíranou oblast do posledních detailů. Proto budou základní možnosti jednotlivých aplikací, které lze použít pro testování a ověřování přítomnosti určitého typu zranitelných míst, v této knize jenom nastíněny a ukázány.

Cílem knihy je také rozvoj produktivního myšlení. Produktivní myšlení je schopnost s využitím získaných informací tvořivě přistupovat k řešení různých předkládaných problémů.

Reproduktivní řešení není v tomto případě možné, jelikož se nejedná o problémy, které by se v nějaké významné míře opakovaly.

V dnešní době jsou poznatky o webových aplikacích a drátových a bezdrátových sítích snadno dostupné a možnosti nalezení a zneužití bezpečnostních mezer jsou velké. Problematika probíraná v dalších kapitolách bude tedy jen náhledem do dané oblasti. Odkazy na detailnější literaturu najdete v referencích na konci každé kapitoly.

Fáze 4: Report

V poslední fázi každé kapitoly bude stručně nastíněna forma reportu, který by měl sumarizovat výsledky jednotlivých testů a případně přidat také zjištění a poznatky, které byly při testování získány.

V textu se vyskytuje také text psaný kurzivou. Jedná se o komentář autora, který není myšlen jako běžná součást předkládaného reportu. Slouží pouze čtenáři pro vysvětlení a objasnění zvolených položek a uvedených informací.

Penetrační testování

V této části textu bude zodpovězeno několik základních otázek týkajících se penetračního testování.

Otázka: Proč jsou penetrační testy důležité?

Společnost Ponemon Institute provedla ve čtyřech evropských zemích (ve Velké Británii, v Německu, ve Francii a v Itálii) studii s názvem 2011 Cost of Data Breach Study [1], kterou analyzovala výšku finančních ztrát způsobených odcizením interních a citlivých firemních dokumentů. Ve studii byly analyzovány také četnosti příčin, které firmy uvádějí jako hlavní důvod ztráty a odcizení citlivých dat. Následující tabulka 1.1 prezentuje část výsledků, které z dané studie vyplynuly.

Tabulka 1.1 Cena ztráty dat

	Německo	Velká Británie	Francie	Itálie
Podnikatelské finanční ztráty	1,33 mil. €	780 tis. £	782 tis. €	474 tis. €
Průměrné finanční ztráty na jednotku	146 €	79 £	122 €	78 €
Procento zákazníků, kteří opustí společnost po ztrátě	3,5 %	2,9 %	4,4 %	3,5 %
Statistika příčin ztráty dat:				
Kriminální útoky a krádeže	42 %	31 %	43 %	28 %
Nedbalost zaměstnanců a dodavatelů	38 %	36 %	30 %	39 %
Selhání IT a byznys procesů	19 %	33 %	26 %	33 %

Odkazy na původní znění výsledků z provedené studie v jednotlivých zemích (v pořadí uvedených zleva) lze najít v referencích pod čísly [1], [2], [3] a [4].

Z prezentovaných výsledků studie vyplývá, že ztráty nejsou zanedbatelné. Realizací penetračních testů firemní sítě (Wi-Fi i klasické drátové) se ověřuje úroveň jejího zabezpečení, která se ve výše uvedené studii také podílela na vzniklých finančních ztrátách. Testy by měly ověřit odolnost jak vůči útokům z vnějšího světa, tak vůči útokům vlastních zaměstnanců,

kteří mají nekalé úmysly. Výsledky těchto testů je pak možné použít jako důkaz důvěryhodnosti pro potenciální investory, obchodní partnery, případné akvizice a fúze či certifikace.

Penetrační testy mohou být nápomocné při stanovování priorit v rámci řešení problémů v IT infrastruktuře. Mohou posloužit při hodnocení efektivnosti ochrany sítě a při určování, které prostředky a zařízení je třeba aktualizovat nebo nahradit novými.

Otázka: Co je cílem penetračního testování?

Jak již bylo uvedeno výše, může to být ověření úrovně zabezpečení. Na tomto místě je ale vhodné poznamenat, že nelze odhalit všechna zranitelná místa. Možnosti jsou totiž značně limitovány přidělenými prostředky (finance, čas, personál). Proto je třeba se zaměřit hlavně na ta zranitelná místa a chyby, které pro společnost představují největší riziko.

Objekty penetračních testů

Otázka: Co by mělo být podrobeno penetračnímu testování?

Testovacímu procesu by mělo podléhat vše, u čeho hrozí riziko nežádoucího průniku do systému, odcizení dat nebo způsobení škody z pohledu podnikatelské aktivity. Tím jsou například myšleny:

- veřejné webové stránky,
- interní informace o zaměstnancích a firemních klientech,
- e-mailové servery a schránky,
- přístupová hesla,
- úložiště dat a FTP servery,
- softwarové aplikace a informační systémy.

Penetrační testy webových aplikací, k jejichž cílové uživatelské skupině patří zákazníci, jsou určitým způsobem nutností. Uživatelé si požadavky a potřeby bezpečnosti nemusí uvědomovat, určitě však nikdo z nich nechce při používání webové aplikace přijít o svoji identitu, soukromé a citlivé údaje a peníze. Uživatelé aplikací tvoří klientelu firmy, takže případné škody a úniky klientských dat způsobují firmě škody, kazí jí pověst a snižují její hodnotu.

Typy testů

Otázka: Jaké typy penetračních testů existují?

Testování slouží pro eliminaci chyb při vývoji systémů a aplikací. Tyto chyby byly většinou neúmyslné. V oblasti informačních technologií lze testy rozdělit do několika základních kategorií podle způsobu provedení na:

- manuální testy,
- automatizované testy,
- semiautomatické testy.

Další dělení podle úrovně znalostí o testovaném systému:

- black-box testy,
- white-box testy,
- grey-box testy.

V další části textu budou popsány jednotlivé typy testů.

Manuální testy

Manuální testy jsou testerem vykonávány manuálně. Mezi výhodami lze klasifikovat možnost vytvořit sofistikované procedury a testy na míru pro specifické podmínky, což automatické testy někdy nedokážou. Další velkou výhodou manuálních testů je, že je provádí člověk a ten umí popsat, co, jak a proč testuje. Výsledky je schopen interpretovat i nezainteresovaným osobám, které nemají o dané oblasti potřebné znalosti (top management, vedení atd.).

Za nevýhody je možné považovat časovou a znalostní náročnost. Vzhledem k téměř neomezeným možnostem, jak například vytvořit webovou aplikaci, jsou nezbytné rozsáhlé znalosti testované oblasti (HTML, SQL, JavaScript atd.). Časová náročnost je dále způsobena manuálním prováděním testů.

Automatizované testy

Automatizované penetrační testy nabízejí výhody v rychlosti, možnostech, rozšiřitelnosti podle vlastních potřeb a v relativně jednoduché verifikovatelnosti a reprodukovatelnosti. Nástroje, které se využívají při automatizovaném testování, byly vytvořeny profesionály, kteří v dané oblasti pracují několik let. Další z výhod v porovnání s manuálními testy je kratší čas na zaučení a následnou aplikaci testů v praxi. Je totiž jednodušší (i časově) naučit se používat aplikaci pro provádění testů než pochopit princip celého testu prováděného manuálně.

Mezi nevýhody je možné zařadit neschopnost prezentovat výsledky v uživatelsky přívětivé formě či blíže vysvětlit podrobnosti k danému problému. Pro správnou interpretaci jsou opět nutné znalosti o použité aplikaci a testované oblasti. Další nevýhodou je také nemožnost testovat některé typy zranitelných míst.

Semiautomatické testy

Třetí kategorií jsou semiautomatické testy. Jde o kombinaci automatických a manuálních testů. Představují kompromis mezi oběma formami se snahou o maximální využití výhod obou forem.

Závěrem je třeba připomenout, že žádná forma testů nikdy nepokrývá 100 % kódu, a tudíž ani neodhalí všechna přítomná zranitelná místa.

Black-box testy

Nejpoužívanějším typem testů jsou tzv. black-box testy. Simulují vnější přístup útočníka, který zná jenom vstupy a potenciální výstupy aplikace, ale nikoliv vnitřní strukturu aplikace či sítě. Pro určení vstupů a výstupů testovaného systému je v některých případech nezbytný poměrně rozsáhlý průzkum. Samotná funkcionalita systému je pro testera černou skříňkou (angl. black-box). Protikladem black-box testů jsou tzv. white-box testy.

Výhodou tohoto typu testů je, že v případě testování aplikací a systémů není potřebná znalost použitého programovacího jazyka a není vyžadováno ani zpřístupnění zdrojového kódu, který se často firmy snaží udržet v tajnosti. Další výhodou je vysoká míra variability, tj. možnost přizpůsobit testy na míru požadavkům zadavatele.

Mezi nevýhody lze zařadit potřebu širokých znalostí testera. Dále nemusí být objeveny chyby, které vyžadují sofistikovanější přístupy, a není ověřena efektivita (optimalizace) kódu.

White-box testy

V porovnání s předchozím typem testů (black-box) jsou pro tyto testy typické plné vstupní znalosti. Jsou založeny na znalosti architektury a zdrojového kódu aplikace nebo, v případě počítačových sítí, na znalosti architektury, typu a počtu přítomných zařízení a na firemních politikách. Při testování probíhá analýza zdrojového kódu, v němž se hledají chyby. Takový druh testů vyžaduje znalost použitého programovacího jazyka a dobře napsaný a okomentovaný kód.

Hlavní výhodou je, že znalost kódu nebo struktury sítě umožňuje najít potenciální zranitelná místa v podstatně kratší době při současně podrobnější kompletní analýze. V případě aplikací je přidruženou výhodou také optimalizace kódu, kterou je možné provést na základě nalezených chyb a zranitelných míst.

V případě aplikací je nevýhodou nutná znalost použitého programovacího jazyka, což může v nepřímém důsledku zvýšit cenu testu, jelikož je od testera vyžadována vyšší kvalifikace. Další nevýhodou je časová náročnost a relativně úzké zaměření na kód a architekturu.

Grey-box testy

Alternativou k předchozím dvěma typům testů jsou tzv. grey-box testy. Ty se snaží maximálně využít výhody a přínosy obou výše uvedených typů testů. Při testech se využívají znalosti vnitřní logiky aplikace, ale testy probíhají z hlediska uživatele nebo, v případě bezpečnostních testů, potenciálního útočníka.

Grey-box testy mohou také zahrnovat metody reverzního inženýrství pro určení limitních hodnot vstupních údajů nebo chybových hlášení.

Průběh penetračních testů

Otázka: Jak by měly probíhat penetrační testy?

V současné době existuje několik metodik pro provádění penetračních testů. Komerční společnosti, které provádějí penetrační testování nebo školení a certifikaci tzv. etických hackerů, udržují své metodiky v tajnosti jako své know-how. Naproti tomu existuje také několik opensourcových neboli otevřených a volně dostupných metodik pro testování.

Příkladem takové otevřené metodiky je Open-Source Security Testing Methodology Manual, který je dostupný online na webových stránkách:

Web: `http://isecom.securenetltd.com/osstmm.en.2.1.pdf`

Uvedená metodologie probírá základní oblasti, mezi něž patří například:

- informační bezpečnost,
- procesní bezpečnost,
- bezpečnost síťových technologií,
- komunikační bezpečnost,
- bezpečnost bezdrátových sítí,
- fyzická bezpečnost,
- reportování.

Každá probíraná sekce je rozdělena do několika modulů. V jednotlivých modulech jsou popsány základní informace, co je hlavním cílem, jaké jsou očekávané výsledky, a také obecné základní kroky pro provedení testu. Uvedené kroky popisují, co je vhodné otestovat (nepopisují však způsob testování).

Příklad popisu testovacích bodů pro otestování systému IDS v metodice Open-Source Security Testing Methodology Manual:

IDS a identifikace vlastností

1. *Ověření typu shromážděných informací získaných od IDS*
2. *Posouzení ochrany nebo vlivu IDS na síť*
3. *Otestování IDS pro urgentní stavy*
4. *Otestování nastavení citlivosti podpisu pro více než 1 minutu, 5 minut, 60 minut a 24 hodin*

   Testování konfigurace IDS
5. *Otestování IDS pro nakonfigurování reakcí proti rozmanitým útokům*
6. *Otestování IDS pro nakonfigurování reakcí na tzv. temném URL a zabraňující zpětné analýze využívají zatížení*
7. *Otestování IDS pro nakonfigurování reakcí vůči rychlým úpravám a posílání paketů*

8. *Otestování IDS pro nakonfigurování reakcí vůči náhodným změnám rychlosti úprav v průběhu útoku*
9. *Otestování IDS pro nakonfigurování reakcí vůči náhodným úpravám protokolu během útoku*
10. *Otestování IDS pro nakonfigurování reakcí proti náhodným úpravám zdrojové adresy během útoku*
11. *Otestování IDS pro nakonfigurování reakcí proti úpravám zdrojového portu*
12. *Otestování IDS pro schopnost zvládnout fragmentované pakety*
13. *Otestování IDS pro schopnost řešení specifických útoků systémovou metodou*
14. *Otestování vlivu a reakce IDS proti jedné IP adrese vůči skupině různých IP adres*

    Prohlížení záznamových souborů a varování IDS
15. *Shoda IDS výstrahy o identifikaci jednotlivých zranitelných míst*
16. *Shoda IDS upozornění na prolomení hesla*
17. *Shoda IDS upozornění na testy důvěryhodných systémů*

Obecnou metodologií managementu bezpečnosti informačních systémů se zabývají normy *ISO 27001* a *ISO 27002.* Ty jsou určeny pro organizace, které pracují s informacemi: jedná se například o státní správu, IT služby, softwarové firmy, telekomunikační operátory atd.

Norma ISO 27001 poskytuje model pro zavedení efektivního systému řízení bezpečnosti informací (ISMS) v organizaci a doplňuje tak normu ISO 27002. Obě normy jsou úzce propojeny, každá z nich však plní jinou roli. Zatímco norma ISO 27002 poskytuje podrobný přehled (katalog) bezpečnostních opatření, která mohou být vybrána při budování ISMS, norma ISO 27001 specifikuje požadavky na to, jak ISMS v organizaci správně zavést. Případná certifikace ISMS pak probíhá podle ISO 27001. [7]

Další obecnou metodikou, jak provádět penetrační testy, je *Technical Guide to Information Security Testing and Assessment*, kterou vydal Americký národní institut pro standardizaci a technologie. Je dostupná na webových stránkách:

Web: `http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf`

Organizace OWASP vytvořila metodiku, která je speciálně zaměřená na penetrační testy webových aplikací. Tato metodologie je dostupná na webových stránkách:

Web: `www.owasp.org/images/5/56/OWASP_Testing_Guide_v3.pdf`

Otázka: Jaké jsou právní aspekty penetračního testování?

K průběhu a vykonávání penetračních testů je ještě vhodné poznamenat, že při prolomení zabezpečení systému může být získán přístup k privátním nebo tajným informacím vlastníka

systému. Je proto jednoznačně nutné konzultovat takové testování zabezpečovacích mechanismů s odpovědnými osobami a jejich provedení mít od kompetentních osob písemně schváleno.

Písemné schválení pomůže předejít případným problémům v budoucnosti. Svévolné nebo iniciativní testování se nemusí setkat s pochopením druhé strany, a v některých případech může být klasifikováno dokonce jako trestný čin. Aktuálně (rok 2012) platný zákon č. 40/2009 Sb., trestního zákoníku, část druhá, zvláštní část, § 230 *Neoprávněný přístup k počítačovému systému a nosiči informací* uvádí:

(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(3) Odnětím svobody na šest měsíců až tři léta, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 nebo 2

a) v úmyslu způsobit jinému škodu nebo jinou újmu nebo získat sobě nebo jinému neoprávněný prospěch, nebo

b) v úmyslu neoprávněně omezit funkčnost počítačového systému nebo jiného technického zařízení pro zpracování dat.

(4) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 nebo 2 jako člen organizované skupiny,

b) způsobí-li takovým činem značnou škodu,

c) způsobí-li takovým činem vážnou poruchu v činnosti orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci,

d) získá-li takovým činem pro sebe nebo pro jiného značný prospěch, nebo

e) způsobí-li takovým činem vážnou poruchu v činnosti právnické nebo fyzické osoby, která je podnikatelem.

(5) Odnětím svobody na tři léta až osm let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 nebo 2 škodu velkého rozsahu, nebo

b) získá-li takovým činem pro sebe nebo pro jiného prospěch velkého rozsahu.

Informace o dalších paragrafech lze najít v trestním zákoníku. [5] K výše uvedenému paragrafu trestního zákoníku je třeba poznamenat, že podle stanoviska prof. Smejkala je „pro možnou klasifikaci této činnosti jako trestného činu nezbytné naplnění této skutkové podstaty, znak ‚neoprávněnosti'. To znamená, že se musí jednat o znaky neoprávněného průniku". [6] Samozřejmě se však nelze spoléhat na vlastní tvrzení, že cílem nebylo zneužití získaného přístupu, dat nebo informací a ostatní nelegální činnosti vyjmenované zákonem. Proto je nezbytné písemné vyjádření vlastníka systému/aplikace apod., se všemi potřebnými informacemi, vydané kompetentními osobami z členů vedení. Konzultace s právním oddělením je namístě zejména v případech, kdy chybějí jakékoliv zkušenosti s touto problematikou.

Otázka: Do jaké míry je potřeba testovat?

Na tuto otázku by bylo možné odpovědět: Nikdy to není dost! To ale z praktického hlediska není možné. Jak jsme již uvedli výše, cílem penetračních testů je ověření úrovně zabezpečení. S každým dalším testem, kterým testujeme bezpečnost, ale klesá jeho marginální přínos – každý další test tedy přináší méně nových a hodnotných informací než předchozí.

Proto je třeba zvolit správný počet provedených testů. Rostoucí rozsáhlost a detailnost testů zvyšuje cenu celého testovacího procesu.

Každý provedený test, který přináší informace pod hranicí s požadovanou informační hodnotou, je v podstatě zbytečný a vytváří přímé i nepřímé náklady vynaložené navíc. Stanovení hranice informační hodnoty získaných výsledků je jedna z tacitních znalostí, tj. znalost, která se nedá získat jinak než životními zkušenostmi.

Obvykle se tzv. hloubka testů určuje například určitou úrovní dosažení oprávnění, získání určitých dat, přístupu k aplikaci nebo systému.

Hloubka testu také závisí na finální sumě peněz, která má být investována do zabezpečení a jeho testování. Dalším faktorem, na němž závisí investovaná suma a potřeba testování, je velikost rizika, resp. pravděpodobnost, že nastane problémová situace – dojde k průniku do sítě, k odcizení informací atd. Když bude například toto potenciální riziko průniku kvantitativně ohodnoceno na dva miliony korun, firma nebude investovat do zabezpečení a jeho testování více než čtvrtinu až třetinu hodnoty rizika. [10]

Nástroje pro testování

Otázka: Jakými nástroji testovat?

Penetračnímu testování může být podrobena reálná již hotová a používaná infrastruktura / webová aplikace / informační systém / server, nebo může jít o teprve vyvíjenou a připravovanou infrastrukturu / webovou aplikaci / informační systém / server. Pro testování je nutné hardwarové a softwarové vybavení.

V dnešní době nejsou při spuštění testů problémem hardwarové prostředky. Hardware je běžně dostupný a jeho cena je relativně nízká. Jedinou problémovou oblast v rámci hardwaru představuje typ síťového zařízení. Je nezbytné, aby ovladače zařízení podporovaly práci v promiskuitním módu. Ověření podpory a nastavení promiskuitního módu bude blíže popsáno v jednotlivých testech, kde jsou tato nastavení potřeba.

Co se týče softwarového vybavení, existuje několik desítek předem připravených prostředí, která obsahují několik desítek nástrojů pro různé druhy testů. Z množství testovacích prostředí stojí za zmínku například:

- BackTrack Linux – **Web:** `www.backtrack-linux.org`
- Fedora Security Spin – **Web:** `http://spins.fedoraproject.org/security`
- KATANA – **Web:** `www.hackfromacave.com/katana.html`
- Pentoo – **Web:** `www.pentoo.ch`
- BlackBuntu – **Web:** `www.blackbuntu.com`
- Matriux – **Web:** `www.matriux.com`
- OWASP Web Testing Environment (WTE) – **Web:** `http://appseclive.org`
- Live Hacking CD – **Web:** `www.livehacking.com/live-hacking-cd`
- Samurai Web testing Framework – **Web:** `http://samurai.inguardians.com`
- The Open Web Application Security Project (OWASP) – **Web:** `www.owasp.org/index.php/Category:OWASP_Live_CD_Project`
- Organizational System Wireless Auditor Asistent (OSWA) – **Web:** `http://securitystartshere.org/page-training-oswa-assistant.htm`

Všechny výše uvedené distribuce obsahují nástroje pro penetrační testování. Některé z nich se specializují například na testování bezdrátových sítí (OSWA) nebo webových aplikací (Samurai WTF či OWASP). Některá prostředí z výše uvedeného seznamu budou používána v dalších kapitolách knihy.

Distribuce lze stáhnout ve formátu LiveCD nebo LiveDVD, který lze po klasickém „vypálení" na CD nebo DVD použít jako bootovatelné médium, tzn. že po vložení CD/DVD do mechaniky a následném restartu stanice dojde k nabootování distribuce určené pro penetrační testování.

Specialitou je vytvoření bootovatelných USB disků. Pro vytvoření je vhodné použít aplikaci s názvem Unetbootin, která je volně dostupná na webových stránkách:

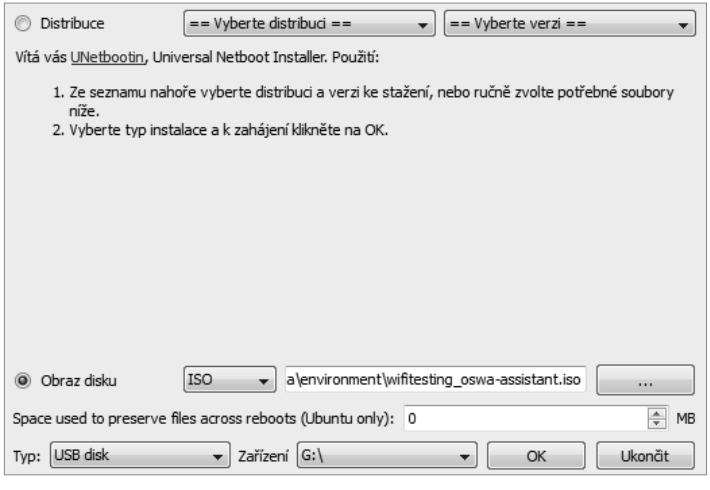
Web: `http://unetbootin.sourceforge.net`

Uvedenou aplikaci je možné používat na operačních systémech Windows, Linux a Mac OS X. Není vyžadována instalace a po stažení je možné ji začít hned používat.

Vytvoření bootovatelného USB disku popisuje následující postup:

1. Stáhněte si aplikaci Unetbootin.
2. Připojte USB disk o minimální volné kapacitě 2 GB.
3. Stáhněte obraz požadované distribuce určené pro penetrační testování.
4. Spusťte aplikaci Unetbootin.
5. Zvolte možnost Obraz disku (viz obrázek 1.1).
6. Prostřednictvím tlačítka **[...]** vyberte obraz testovací distribuce.
7. Zvolte požadovanou jednotku USB disku.
8. Potvrďte výběr a nastavení tlačítkem **OK**.
9. Následně dojde k vytvoření bootovatelneho USB disku se zvolenou distribucí.

Nyní je pouze nutné nastavit v systému jako primární bootovací jednotku USB rozhraní a restartovat počítač.



Obrázek 1.1 Unetbootin

V některých případech výše uvedených testovacích distribucí je nabízeno stažení ve formátu obrazů (image), které lze importovat do virtualizační aplikace, jako je VMware Workstation, VMware Player (`www.vmware.com`) nebo VirutalBox (`www.virtualbox.org`).

Import do aplikací VMware je možný přes menu:

File → Open virutal machine → najít a zvolit soubor s příponou .vmx

Import do aplikace VirtualBox je možný přes menu:

File → Import Appliance → Select → najít a zvolit soubor s příponou .ovf

Po výběru daného obrazu virtuálního stroje dojde k načtení jeho konfigurace a následně je možné systém spustit a pracovat s ním jako s normální skutečnou (fyzickou) stanicí.

V některých případech jsou ale tato virtualizační zařízení limitována a neumožňují nahrazovat skutečné fyzické stroje. Problémovou oblastí může být například virtuální síťové zařízení, kde bývá problém s ovladači nebo nabízenými funkcemi. Chování virtualizovaného hardwaru se mírně odlišuje od chování fyzického hardwaru a mohou se objevit specifické problémy, které jsou způsobeny právě virtualizací. Daná problematika však přesahuje rámec této knihy, proto se jí dále nebudeme věnovat.

Výhodou těchto virtuálních obrazů je možnost rychle a pohodlně vytvářet snapshoty – obrazy, které zachycují aktuální stav systému. V případě, že dojde v systému ke změně konfigurace nebo k ireverzibilním poruchám, lze se v případě potřeby vrátit do uložené (funkční) konfigurace.

Nevýhodou těchto virutálních obrazů může být, jak už bylo zmíněno výše, problém s podporou hardwaru, zejména síťových karet, rychlost a výpočetní výkon, který je sdílen s reálnou hardwarovou stanicí.

V průběhu samotného testování někdy přijdou vhod aplikace pro:

- tvorbu videa – v případě potřeby natočit složitější sekvenci kroků pro uvození daného problému nebo jako názornou ukázku určitého problému. Někdy má desetisekundové video vyšší informační hodnotu než dvě stránky textu.
- tvorbu a editaci screenshotů – názorné ukázky jsou velice vhodné, ne vždy si totiž programátor nebo zadavatel, který výsledky studuje, dokáže správně představit, co je daným popisem myšleno. Usnadňuje to interpretaci výsledků nálezů. Vhodnou funkcí je, když aplikace umí kreslit šipky a různé geometrické tvary, u kterých je možné měnit barvu. Tyto kreslicí prvky je vhodné používat pro zvýraznění elementů, na něž se má upřít pozornost. Viz například obrázek 1.2.

Obrázek 1.2 Zvýraznění objektů

- Textové editory pro poznámky a editaci kódu (HTML, XML atd.) – je vhodné si zapisovat poznámky a nálezy, případné nové myšlenky, přístupové údaje, odkazy, vygenerované chyby, dlouhé textové a číselné řetězce, postupně sepisovat shrnutí a závěrečnou zprávu. Ne vždy si člověk pamatuje objevené detaily i o několik dní, nebo dokonce měsíců později. Pokročilejší textové editory umí používat regulární výrazy, čímž značně zrychlují prohledávání a filtrování informací v souborech. Další z funkcí, která může být užitečná, je například hromadná editace souborů nebo porovnávání dvou souborů podle řádků.
- Souborový manažer – usnadňuje operaci se soubory a složkami, v některých případech umožňuje synchronizaci adresářů, binární porovnávání souborů, náhledy na soubory a archivy a podobné funkce. Souborový manažer umožňuje provádět uvedené operace (a mnoho dalších) s větší efektivitou, než by tomu bylo při normálním provádění bez něj.

Metodologie reportu

Proces testování je limitován množstvím dostupných peněz, časem, pracovními silami. Ohraničení testů může být určeno například časově, kdy jsou na ně vyhrazeny kupříkladu tři dny práce v pěti lidech. Závěry penetračních testů by měly být shrnuty ve zprávě, která bude následně předána zadavateli.

Na tomto místě je vhodné upozornit, že negativní výsledek testů může znamenat dobře zabezpečený systém, což ale nepředstavuje neprolomitelnou ochranu. Negativní výsledek může také znamenat špatné navržení testu nebo jeho povrchnost a nedůkladnost.

Další věcí týkající se reportu je zejména způsob komunikace. Při tvorbě výstupních zpráv je důležité vědět, co říct, ale hlavně jak to říct. Jako téměř ve všech oblastech, i v oblasti penetračního testování je důležitá mezilidská komunikace. Při nalezení problémů a chyb v aplikacích, konfiguracích a systémech je potřeba nález oznámit tvůrci/autorovi nebo odpovědné osobě, která by měla zabezpečit nápravu. Zde je vhodné poznamenat, že slušné jednání je velmi důležitou zásadou, na kterou je nutné pamatovat.

Nalezená chyba spočívá většinou v práci nebo myšlení osoby, jejíž pracovní výsledky jsou testovány. K přijetí negativní kritiky dochází jen s velkými obtížemi, obzvlášť je-li podána útočným způsobem. Jak by to NEMĚLO vypadat:

Funkce přihlašování se nedá použít, obzvlášť v prohlížeči Opera to nefunguje. Udělejte s tím něco. S takovým produktem se nedá pracovat.

Takové sdělení by určitě nikomu nepřidalo na pracovním elánu. Proto je vhodné zvolit jinou formu, například následující:

Dobrý den. Prosím vás, mohli byste se podívat na funkci přihlašování? Během testování jsem narazil na problém v prohlížeči Opera verze 10. Po potvrzení přihlašovacích údajů jsem dostal odpověď:

HTTP method GET is not supported by this URL

V případě potřeby dodatečných informací mě neváhejte kontaktovat, rád vám dodám všechny potřebné podklady.

Výše uvedené informace o slušnosti při komunikaci se mohou zdát samozřejmostí, ale bohužel tomu tak v praxi vždy není.

Report by měl být odevzdán v souborovém formátu, u kterého lze předpokládat, že jej nabyvatel nebude mít problém otevřít. Nejčastěji se jedná o formáty dokumentů balíku Office nebo univerzální formát PDF. Specifikace souborového formátu výstupního reportu může být také součástí zadání, interní směrnice nebo smlouvy.

Vzdělávání a trénink

V dnešní době může téměř každý, kdo má zájem, získat ohromné množství informací z různých oborů. Informace jsou dostupné v:

- tištěné podobě – knihy, časopisy,
- elektronické podobě – internetové stránky, diskusní fóra, e-knihy, e-časopisy,
- interaktivní podobě – konference, semináře, přednášky, workshopy.

Následující stránky této kapitoly jsou věnovány několika ukázkovým projektům, kde lze takové informace zejména z oboru IT bezpečnosti získat.

ICT Security

ICT SECURITY je český odborný online magazín zaměřený na bezpečnostní problematiku informačních technologií, dostupný na webových stránkách:

Web: `www.ictsecurity.cz`

V prezentovaných článcích lze najít kromě informací od odborníků z dané oblasti také tipy a návody pro zabezpečení firemní sítě. Magazín umožňuje s pomocí čtenářských dotazů diskutovat s odborníky o reálných problémech z praxe.

SystemOnline

Dalším z magazínů, který se zabývá problematikou bezpečností IT technologií, sleduje moderní trendy a vede o nich diskuse, je sekce IT Security magazínu SystemOnline. Magazín je dostupný na webových stránkách:

Web: `www.systemonline.cz/it-security`

ANOPRESS IT

ANOPRESS IT je databáze monitoringu médií a časopisových článků českých, slovenských a zahraničních médií. Přístup do systému vyžaduje placenou registraci.

Web: `www.anopress.cz`

Databáze obsahuje reportáže a články monitorovaných médií, mezi která patří z oblasti IT například: CDR, Computerworld, Connect!, DigiWeb, Chip, Interval, Lupa, Mobil, Mobility, PC World, Softwarové noviny, Svět hardware, Svět sítí, Underground, Computer, ChannelWorld, CHIP, IT CAD, IT Systems, Počítač pro každého, Professional Computing Speciál, Reseller Magazine, Security World, businessit, Businessworld, Hdworld, iDnes – Technika, NetShopper, PCWorld, Root, Securityworld nebo Živě.

IT Security Workshop

V roce 2012 se konal šestý ročník akce s názvem IT Security Workshop s podtitulem Bezpečnost dat a sítí. Jeho hlavním cílem je seznámit odborníky pracující na vytváření a řízení informační bezpečnosti firemních sítí s riziky v oblasti ochrany dat a s možnostmi, jak tato rizika snižovat.

Bližší informace je možné získat na webových stránkách:

Web: `www.itsw.cz`

Security Session

Na brněnské Fakultě informatiky VUT je každoročně organizována konference zaměřená na šíření osvěty v oblasti informační bezpečnosti a potenciálních hrozeb. Informace o jednotlivých ročnících je možné získat na webových stránkách:

Web: `http://session.security-portal.cz`

Na posledním ročníku (2012) byla probírána témata jako ochrana proti DoS útokům, Exploity nebo Host Intrusion Prevention systémy.

V návaznosti na tyto přednášky je vhodné poznamenat, že existuje také několik projektů, které jsou zaměřeny na výuku v distanční podobě. Zájemce může studovat online s pomocí videí a interaktivních prostředí; mezi nejznámější e-learningové kurzy patří kurzy od společnosti Cisco. Některé formy vzdělávání jsou placené. Jako alternativa k těmto komerčním variantám ale existují také volně dostupné materiály a kurzy.

Google Code University

Společnost Google realizuje v rámci šíření osvěty projekt pod názvem Google Code University (GCU).

Web: `http://code.google.com/intl/cs/edu`

Tato distanční univerzita nabízí několik videotutoriálů a instruktážních materiálů zaměřených například na:

- programovací jazyky – C++, Java, Ajax,
- programování webu – CSS, HTML, JavaScript,
- webovou bezpečnost,
- Android,
- algoritmizaci.

Jednou z možností interakce s ostatními studenty je diskusní fórum, kde si mohou účastníci vyměňovat zkušenosti a diskutovat o řešení nejen probíraných problémů. Přístup k těmto materiálům nevyžaduje registraci. Specialitou je vyhledávací funkce, která umožňuje vyhledávat vzdělávací materiály z různých IT oblastí (viz obrázek 1.3).

Obrázek 1.3 GSU – vyhledávání materiálů

Microsoft Virtual Academy

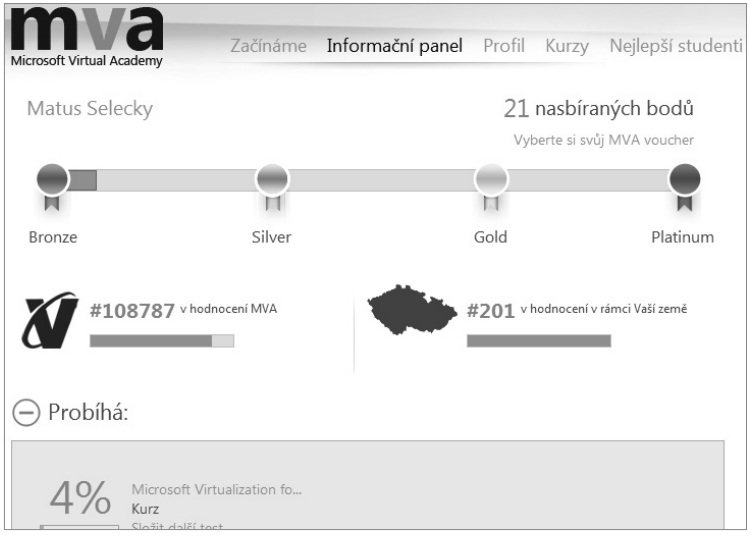
Společnost Microsoft vytvořila v rámci snahy o propagaci svých platforem a výchovu budoucích odborníků pro své systémy projekt virutální akademie. Je dostupný na webových stránkách:

Web: `www.microsoftvirtualacademy.com/Home.aspx`

Přístup k materiálům je bezplatný, vyžadována je pouze registrace. Akademie nabízí videotutoriály na aktuální témata z oblasti technologických novinek společnosti Microsoft. Mezi novinkami je možné najít například:

- Microsoft's Private Cloud,
- virutalizaci ve VMware,
- System Center 2012,
- Windows Server 8,
- Windows Azure,
- SQL Azure
- a další.

Tutoriály obsahují několik částí, přičemž pro postup do vyšších úrovní je na konci jednotlivých sekcí vyžadováno splnění krátkého testu. Po úspěšném absolvování tutoriálu získává student body, které ho umísťují v žebříčku nejlepších studentů z celého světa nebo vlastní země.



Obrázek 1.4 Microsoft Virtual Academy