

**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

Matůš 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.

© Albatros Media a. s. Všechna práva vyhrazena. Žádná část této publikace nesmí být kopírována a rozmnožována za účelem rozšiřování v jakékoli formě či jakýmkoli způsobem bez písemného souhlasu vydavatele.

1. vydání

 **ALBATROS** MEDIA a.s.

Obsah

	3
Předmluva autora	7
Co obsahuje tato kniha	7
Zpětná vazba od čtenářů	9
Errata	10
KAPITOLA 1	
Metodologie a nástroje penetračních testů	11
Úvod	11
Metodologie testování	12
Penetrační testování	14
Typy testů	15
Průběh penetračních testů	18
Nástroje pro testování	22
Metodologie reportu	25
Vzdělávání a trénink	26
Závěr	36
Reference	37
KAPITOLA 2	
Externí penetrační testy firemních sítí	39
Úvod	39
Případová studie	40
Fáze 1: Cíl a rozsah penetračního testu	40
Fáze 2: Sběr dat	44
Fáze 3: Skenování a exploitace	65
Fáze 4: Report	92
Závěr	95
Reference	97

KAPITOLA 3

Interní penetrační testy firemních sítí	99
Úvod	99
Případová studie	100
Fáze 1: Cíl a rozsah penetračního testu	101
Fáze 2: Sběr dat	103
Fáze 3: Skenování a exploitace	116
Fáze 4: Report	151
Závěr	154
Reference	156

KAPITOLA 4

Penetrační testy bezdrátových sítí	159
Úvod	159
Případová studie	160
Fáze 1: Cíl a rozsah penetračního testu	161
Vnější testování	162
Vnitřní testování	162
Fáze 2: Sběr dat	163
Příprava	163
Testování	165
Fáze 3: Skenování a exploitace	170
I. Vnější testování	171
II. Vnitřní testování	190
Fáze 4: Report	220
Závěr	224
Reference	226

KAPITOLA 5

Penetrační testy webových aplikací	229
Úvod	229
Případová studie	230
Fáze 1: Cíl a rozsah penetračního testu	231
Zranitelné místo: Injekce	231
Zranitelné místo: Cross-Site Scripting (XSS)	232
Zranitelné místo: Zabezpečení autentifikace a managementu relací	233
Zranitelné místo: Zabezpečení přímého odkazu na objekt	233
Fáze 2: Sběr dat	234
Průzkum veřejně dostupných informací	236
Analýza adresářové struktury serveru	237
Identifikování všech relevantních vstupů	240
Zjištění verzí serverových systémů	241
Fáze 3: Skenování a exploitace	242
Zranitelné místo: Injektování SQL a LDAP kódu	242
Zranitelné místo: XSS	258
Zranitelné místo: Zabezpečení autentifikace a managementu relací	271
Zranitelné místo: Zabezpečení přímého odkazu na objekt	278
Dodatek na závěr	282
Další inspirace	288
Fáze 4: Report	290
Závěr	293
Reference	295
Rejstřík	297

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 nabízel 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 videoseverech, 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 referenci 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, jež 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 uživatelé 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.

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 konfiguračním aplikacím a k informacím o uživateli? 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. Tato 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 exploitate

Třetí fáze obnáší proces skenování testovaného systému, testování zabezpečení a pokusy o prolomení bezpečnostních mechanismů. Hlavním cílem exploitate může být například získání přístupu do systému nebo databáze bez validních přihlašovacích údajů, získání citlivých informací o uživateli 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 webových aplikací 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 funkcionality 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.securenet1td.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 využívající 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